

QNAP Turbo NAS
Software User Manual
(Version: 3.8)

© 2013 QNAP Systems, Inc. All Rights Reserved.

Table of Contents

1. Notice	6
1.1 Regulatory Notice.....	7
1.2 Symbols in this document.....	8
1.3 Safety Information and Precautions.....	9
2. Getting Started.....	10
2.1 Browse the CD-ROM.....	16
2.2 Hard Disk Drive Compatibility List.....	18
2.3 Check System Status (LED and Alarm Buzzer).....	19
2.4 Connect to the NAS Network Shares.....	22
2.5 Connect to the NAS by a Web Browser.....	24
2.6 System Migration.....	30
3. System Administration.....	33
3.1 General Settings.....	34
3.2 Network.....	38
3.3 Service Binding.....	62
3.4 Hardware.....	64
3.5 Security.....	68
3.6 Notification.....	71
3.7 Power Management.....	78
3.8 Network Recycle Bin.....	80
3.9 Back up/Restore Settings.....	81
3.10 System Logs.....	82
3.11 Firmware Update.....	87
3.12 Restore to Factory Default.....	91
4. Disk Management.....	92
4.1 Volume Management.....	92
4.2 RAID Management.....	96
4.3 Hard Disk S.M.A.R.T.....	122
4.4 Encrypted File System.....	123
4.5 iSCSI.....	132
4.5.1 Portal Management.....	132
4.5.2 Target Management.....	143
4.5.2.1 Connect to the iSCSI targets by Microsoft iSCSI Initiator on Windows.....	155
4.5.2.2 Connect to the iSCSI targets by Xtend SAN iSCSI Initiator on Mac OS.....	160
4.5.2.3 Connect to the iSCSI targets by Open-iSCSI Initiator on Ubuntu Linux.....	167
4.5.3 Advanced ACL.....	169
4.5.4 LUN Backup.....	173

4.6 Virtual Disk.....	192
5. Access Right Management.....	197
5.1 Domain Security	197
5.1.1 Join the NAS to Active Directory (Windows Server 2003/2008).....	199
5.1.2 Connect the NAS to an LDAP Directory.....	211
5.2 Users.....	218
5.3 User Groups.....	235
5.4 Share Folders.....	236
5.5 Quota.....	267
6. Network Services.....	268
6.1 Microsoft Networking.....	269
6.2 Apple Networking.....	273
6.3 NFS Service.....	276
6.4 FTP Service.....	279
6.5 Telnet/SSH.....	281
6.6 SNMP Settings	282
6.7 Web Server	284
6.7.1 Virtual Host.....	307
6.8 Network Service Discovery	311
7. Applications	313
7.1 Web File Manager.....	314
7.2 Multimedia Station	332
7.2.1 QMobile.....	363
7.3 Photo Station.....	387
7.4 Music Station.....	413
7.5 HD Station.....	437
7.6 Download Station.....	459
7.7 Surveillance Station	481
7.8 iTunes Server.....	490
7.9 DLNA Media Server.....	493
7.10 MySQL Server.....	494
7.11 QPKG Center	496
7.12 Syslog Server.....	500
7.13 RADIUS Server.....	505
7.14 Backup Server.....	509
7.15 Antivirus.....	513
7.16 TFTP Server.....	523
7.17 VPN Service.....	524
7.18 LDAP Server.....	540

8. Backup	545
8.1 Remote Replication.....	545
8.2 Cloud Backup.....	569
8.3 Time Machine.....	579
8.4 External Drive.....	584
8.5 USB One Touch Copy.....	599
9. External Device	602
9.1 External Storage Device.....	602
9.2 USB Printer.....	612
9.2.1 Windows 7, Vista Users.....	615
9.2.2 Windows XP Users.....	622
9.2.3 Mac OS 10.6.....	624
9.2.4 Mac OS 10.5.....	627
9.2.5 Mac OS 10.4.....	632
9.2.6 Linux (Ubuntu 10.10).....	637
9.3 UPS Settings.....	642
10. MyCloudNAS Service	647
10.1 MyCloudNAS Wizard.....	648
10.2 Configure MyCloudNAS.....	656
10.3 Auto Router Configuration.....	663
11. System Status	666
11.1 System Information.....	666
11.2 System Service.....	667
11.3 Resource Monitor.....	668
12. Use the LCD Panel	672
13. Connect to QNAP NAS from the Internet (DDNS Service)	679
14. Set up SMS, Email, and IM Alert on QNAP NAS	689
15. Set up UPnP Media Server for Media Playing	700
16. Host a Forum with phpBB on QNAP NAS	709
17. NAS Maintenance Settings	721
17.1 System Restart/Shutdown.....	722
17.2 System Temperature Protection.....	725
18. GNU GENERAL PUBLIC LICENSE	726

1. Notice

Thank you for choosing the 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



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.



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 0°C–40°C 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

Web-based Setup of the NAS

To perform system installation without a product CD-ROM, please visit <http://qnap.com/start/en/> and click "Start Now". Follow the on-screen instructions to select your NAS model and finish the hardware and software installation for your OS (Windows, Mac, or Linux). The page also provides access to the download links of QNAP's software utilities and mobile apps.

QNAP English - Global
Hard Disk Compatible List User Manual

Set Up Your Turbo NAS

Store, back up and share your data easily

New to Turbo NAS ?
Follow the steps to get started:

- 1 Set up the hardware for your Turbo NAS
- 2 Install firmware and configure your Turbo NAS
- 3 Get useful tools to enjoy your Turbo NAS

Start Now

Firmware Installation
If you have set up the hardware, please click "Go" to install the Turbo NAS firmware directly.

GO

Enjoy Hands-on Applications for Turbo NAS

Various handy tools are available to smooth your work with the Turbo NAS. You can enjoy convenient data backup, smart download management, remote access to the Turbo NAS anytime and anywhere.

Back up data on your PC
NetBak Replicators
Conveniently back up documents, pictures, music, videos and more to one or multiple Turbo NAS units.
[Learn more](#)
Windows

Access your Turbo NAS easily
MyCloudNAS Connect
3 quick steps to connect to your Turbo NAS with MyCloudNAS Connect via Virtual Private Network (VPN) to manage files by drag-and-drop within Windows Explorer.
[Learn more](#)
Windows

Manage download tasks
QGet
Install QGet to manage BT, HTTP, and FTP download tasks on the Turbo NAS.
[Learn more](#)
Windows Mac Linux

Remote access on the go
Mobile Apps
Access and manage your Turbo NAS and enjoy multimedia files on mobile devices whenever, wherever.
[Learn more](#)
Qfile Qmanager Qmobile

Online Resources Customer Service | Online Support Form | QNAP Forum | User Manual | Tutorials
Facebook Google+ Twitter YouTube

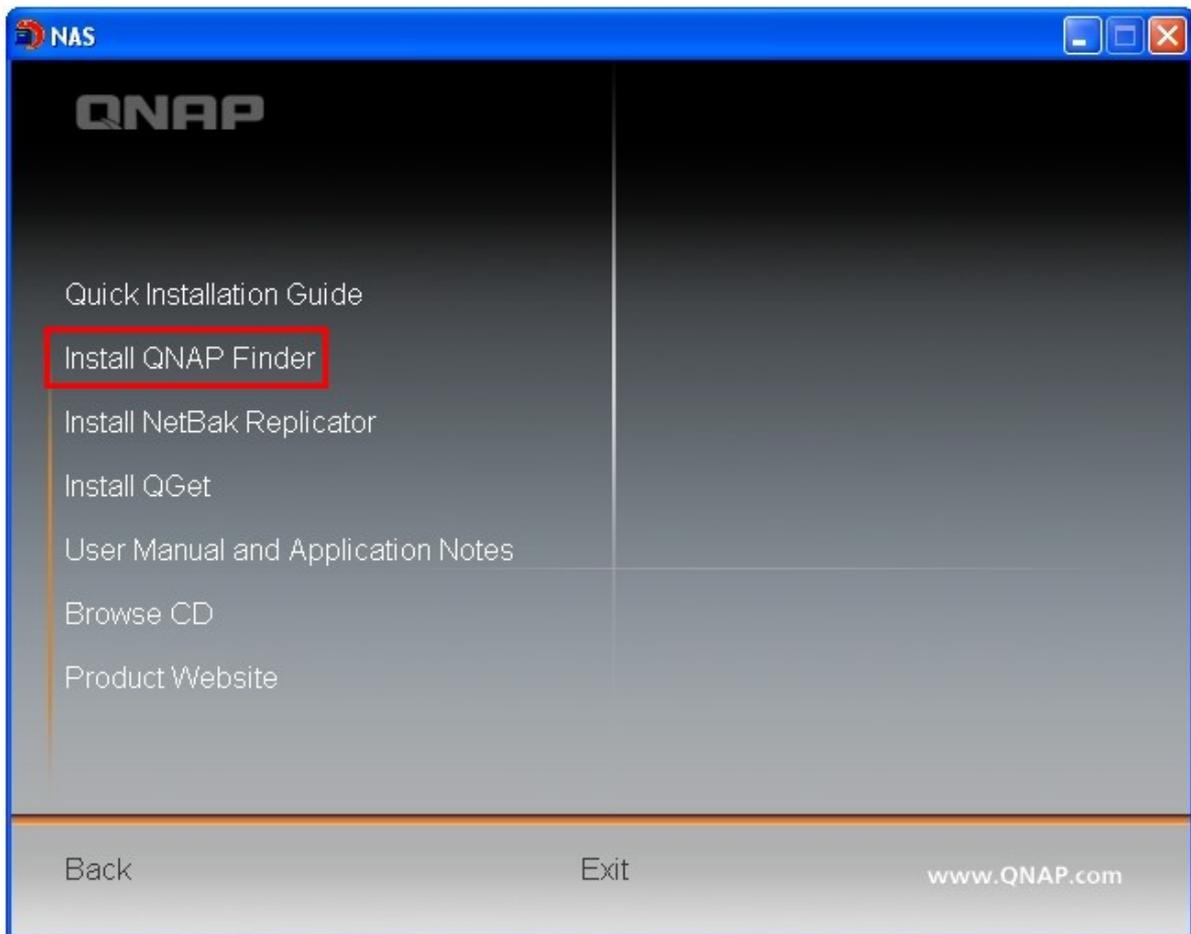
Hardware Installation

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>).

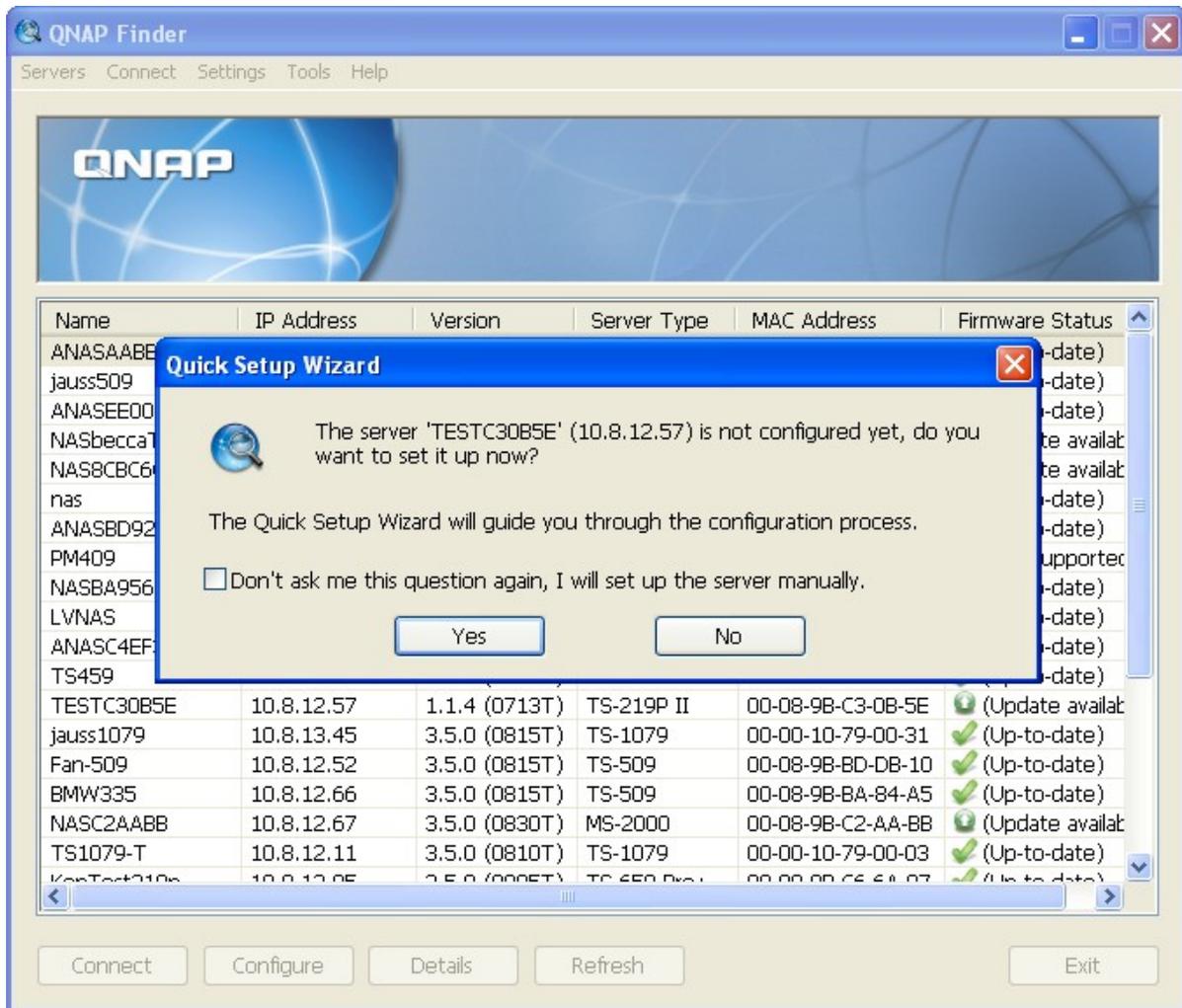
Software Installation (Using the CD-ROM)

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

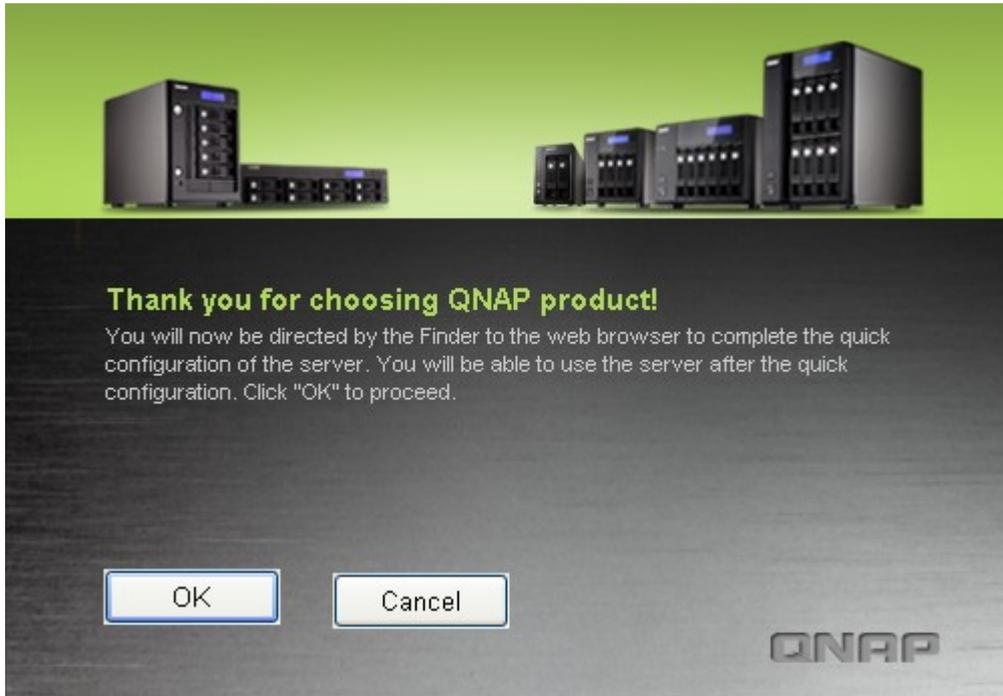
1. Install the QNAP Finder from the product CD-ROM.



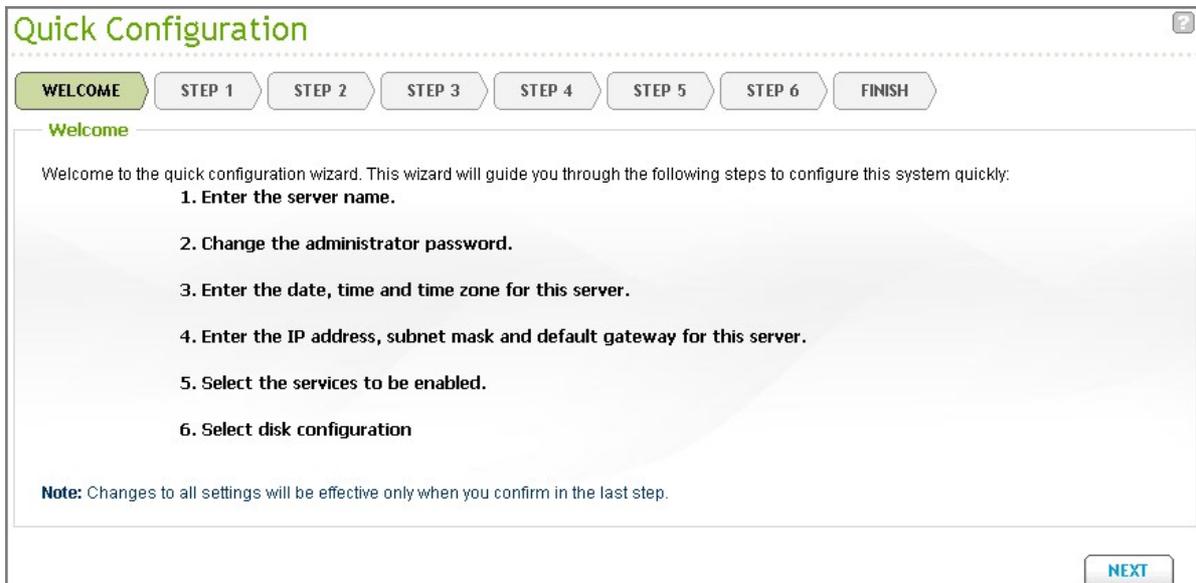
- Run the Finder. If the Finder is blocked by your firewall, unblock the utility.
- The Finder detects the NAS which has not been configured. Click "Yes" to perform quick setup of the NAS.



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.

Quick Configuration

WELCOME STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6 **FINISH**

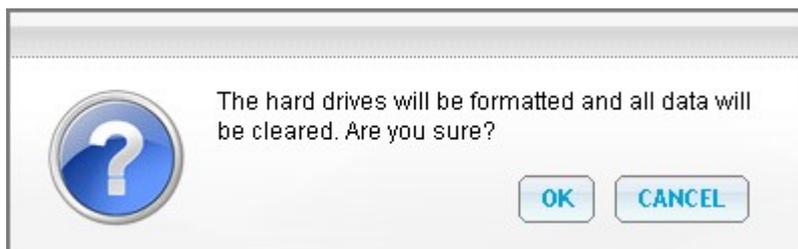
Finish

The changes you have made to the server are as below. Click "Start installation" to begin the quick configuration; or click "Back" to return to the previous steps to modify the settings.

Server Name :	NAS8C8C8C
Password:	The password is unchanged.
Time Zone :	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Time Setting:	Set the server time the same as your computer time.
Network :	Obtain TCP/IP settings automatically via DHCP
IP Address:	--
Subnet Mask:	--
Default Gateway:	--
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Network services:	Microsoft Networking,Web File Manager,FTP Service,Download Station,Multimedia Station,Web Server
Disk configuration:	Raid 1
Encrypt disk volume:	Yes
File System:	EXT4
Drive 1:	Seagate ST3160318AS CC44 149.05 GB
Drive 2:	Seagate ST3160318AS CC44 149.05 GB

BACK **START INSTALLATION**

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



- 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.

Quick Configuration

System is initializing, please wait.

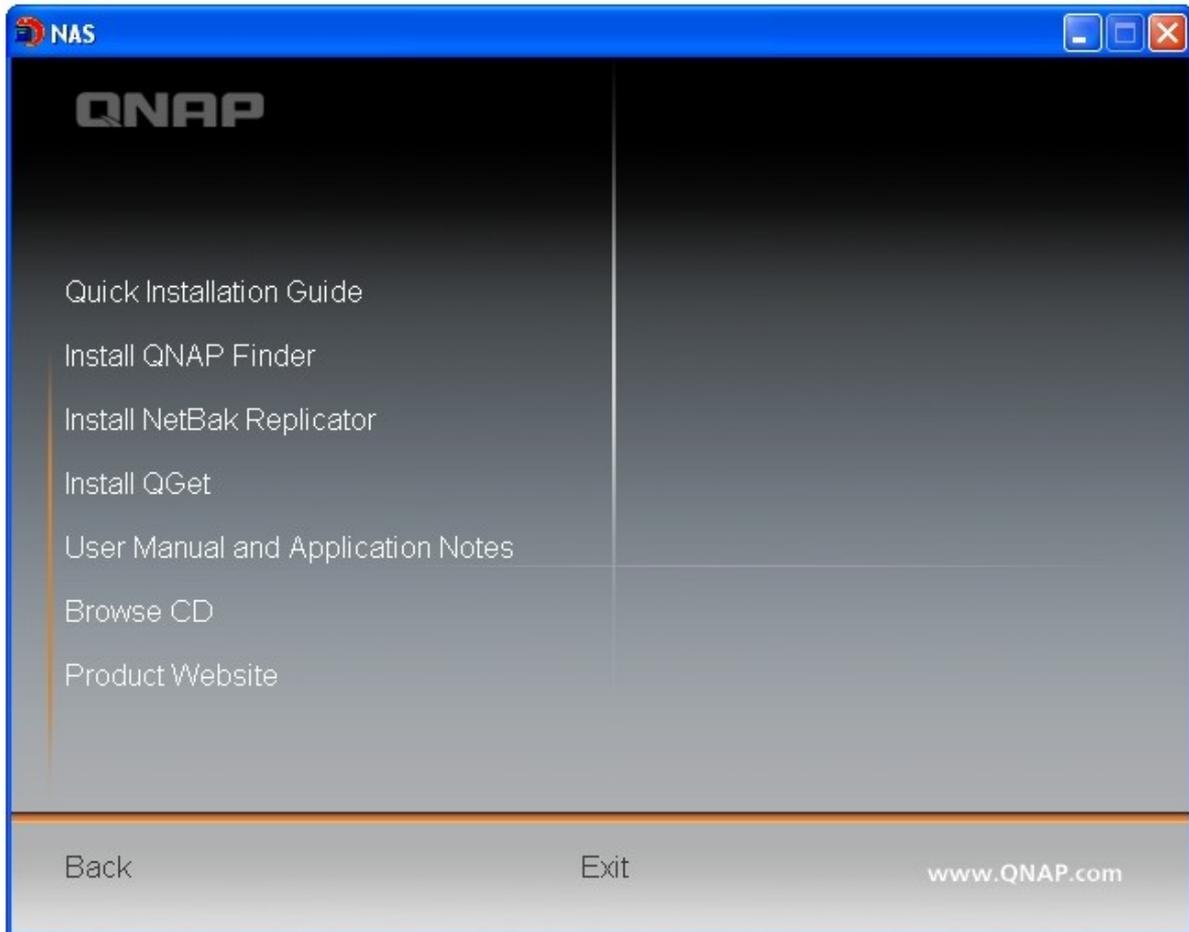
The system is being configured. Do NOT power off the server or unplug the hard drive(s).

-  **1. Change the name for this server.**
-  **2. Change the administrator password.**
-  **3. Change the time settings.**
-  **4. Change the network settings.**
-  **5. Start the network services.**
-  **6. Initialize the hard disk.**

 System configuration completed. [Return to system administration page.](#)

2.1 Browse the CD-ROM

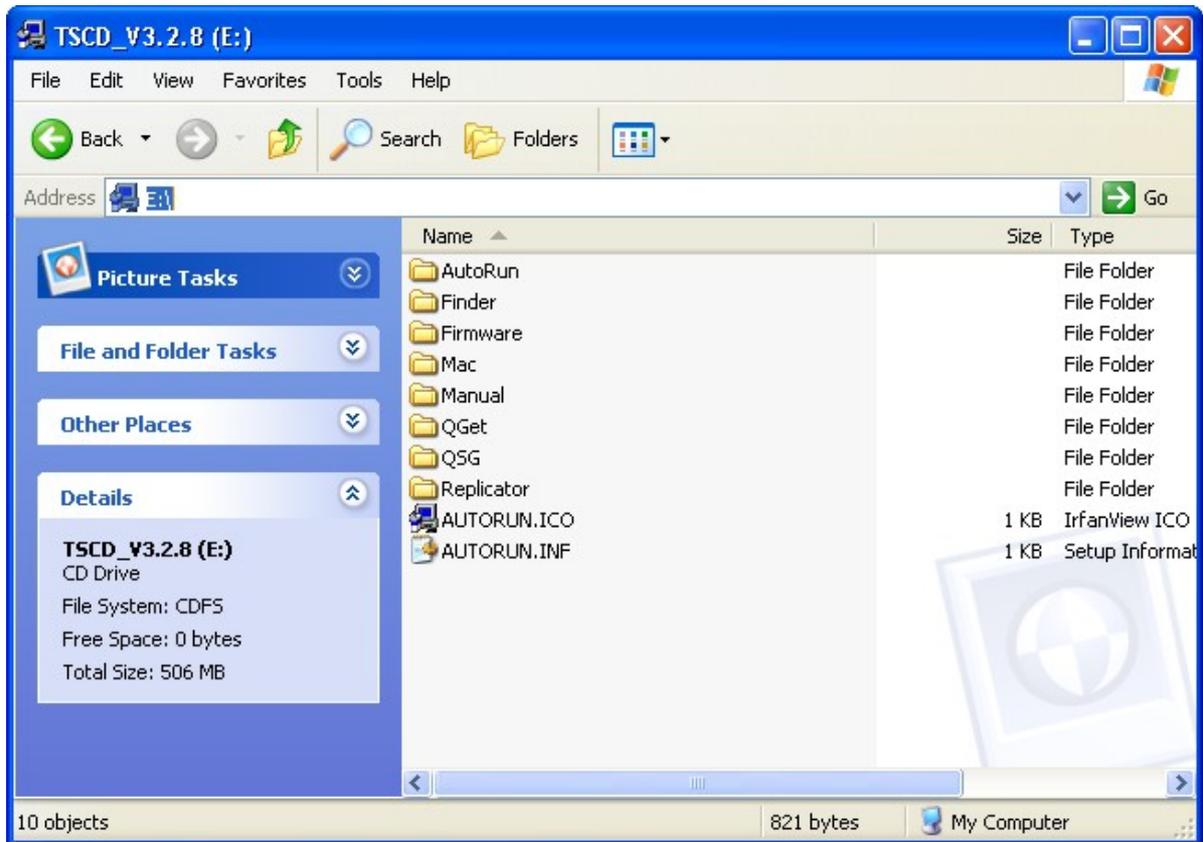
The product CD-ROM contains the documentation including the Quick Installation Guide (QIG), user manual, application notes, and software utilities QNAP Finder, NetBak Replicator, and QGet.



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 the 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 and/or solid-state drives (SSD) 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 from the network 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

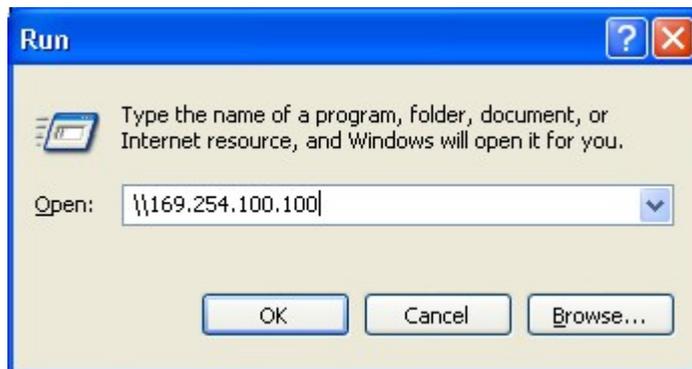
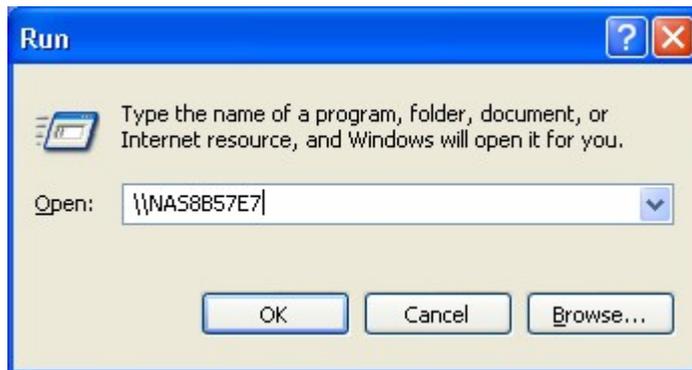
Alarm Buzzer (the alarm buzzer can be disabled in "System Tools" > "Hardware Settings")

Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 username: 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 a Web Browser

To connect to the NAS by a web browser, follow the steps below.

1. Enter `http://NAS IP:8080` or use the Finder to find the NAS and double click the NAS name.

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. Enter the administrator name and password. Turn on the option "Secure login" (Secure Sockets Layer login) to allow secure connection to the NAS. If a user without administration right login the NAS, the user can only change the login password.

Default username: admin
Default password: admin

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



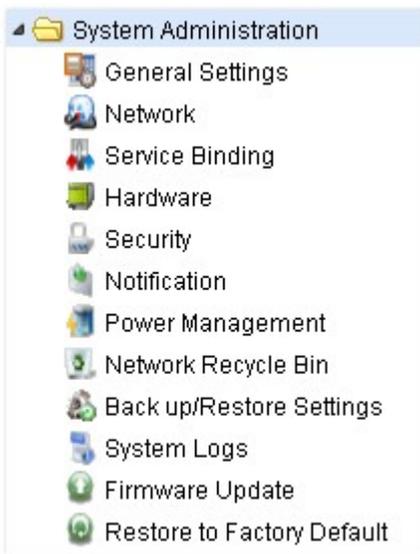
4. The login portal will be shown. Click an application icon to open the service page in the current window or click the + sign of the application icon to open the service page in a new tab.



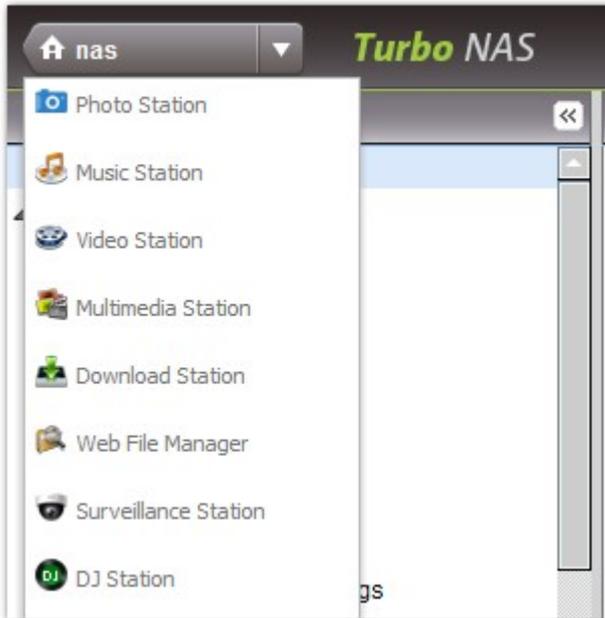
5. To configure the system settings, click "Administration" on the login portal.



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



7. To switch to another application, select the service from the drop-down menu on top of the page.



Click the triangle icon next to the login name on the top right hand for additional options: change the login password, restart/shut down/logout the NAS, or view the product model and firmware version.



2.6 System Migration

Users can migrate their QNAP NAS to another Turbo NAS model with all the data and configuration retained by simply installing the hard drives of the original (source) NAS on the new (destination) NAS according to 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 NAS models which support system migration are listed below.

Source NAS	Destination NAS	Remark
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 NAS should contain enough drive bays to house the hard drives 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 DLNA 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 QPKG's need to be resintalled (e.g. XDove)

3. System Administration

General Settings [34](#)

Network [38](#)

Service Binding [62](#)

Hardware [64](#)

Security [68](#)

Notification [71](#)

Power Management [78](#)

Network Recycle Bin [80](#)

Backup/Restore Settings [81](#)

System Logs [82](#)

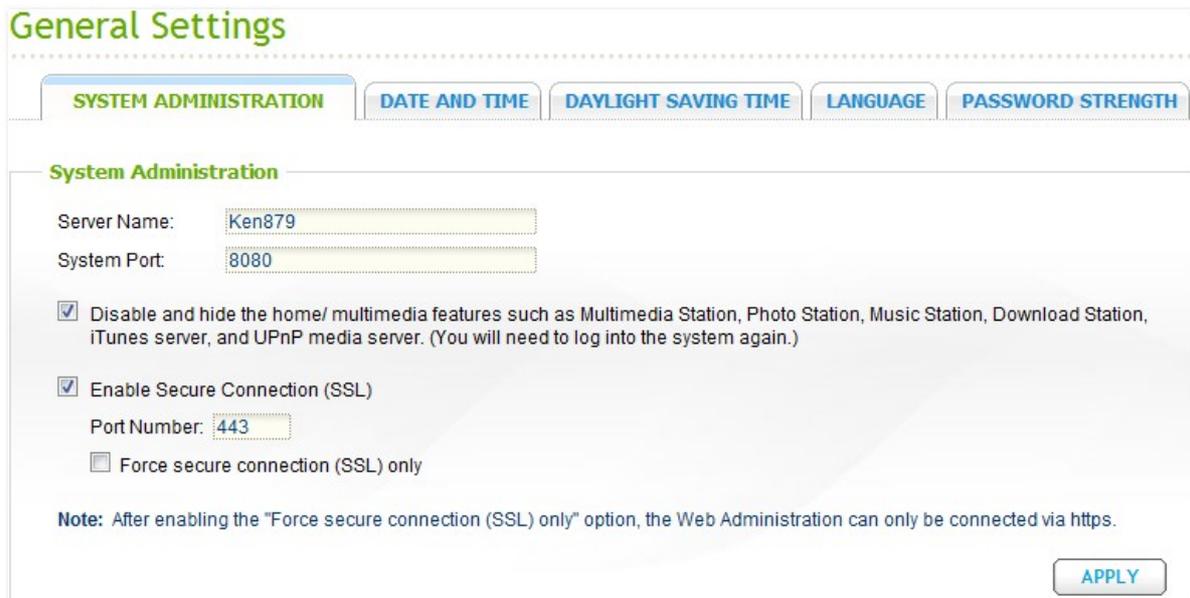
Firmware Update [87](#)

Restore to Factory Default [91](#)

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 screenshot shows the 'General Settings' interface with the 'SYSTEM ADMINISTRATION' tab selected. The 'System Administration' section contains the following fields and options:

- Server Name:
- System Port:
- Disable and hide the home/ multimedia features such as Multimedia Station, Photo Station, Music Station, Download Station, iTunes server, and UPnP media server. (You will need to log into the system again.)
- Enable Secure Connection (SSL)
 - Port Number:
 - Force secure connection (SSL) only

Note: After enabling the "Force secure connection (SSL) only" option, the Web Administration can only be connected via https.

The home/multimedia features such as Multimedia Station, Photo Station, Music Station, Download Station, iTunes server, and DLNA 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.

General Settings

SYSTEM ADMINISTRATION | **DATE AND TIME** | DAYLIGHT SAVING TIME | LANGUAGE | PASSWORD STRENGTH

Current date and time

2010/11/29 12:33:34 Monday

Date and Time

Time Zone: (GMT+08:00) Taipei

Date Format: yyyy/MM/DD

Time Setting: 24HR

Manual Setting

Date/Time: 2010/11/29 / 12 : 31 : 53

Synchronize with an internet time server automatically

Server: pool.ntp.org

Time Interval: 1 day(s)

Set the server time the same as your computer time **UPDATE NOW**

APPLY

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.

General Settings

SYSTEM ADMINISTRATION DATE AND TIME **DAYLIGHT SAVING TIME** LANGUAGE PASSWORD STRENGTH

Daylight Saving Time

Time Zone: **(GMT+08:00) Taipei**

Recent daylight saving time: Start time: --
End time: --

Offset: -- minutes

Adjust system clock automatically for daylight saving time.

Enable customized daylight saving time table.

APPLY

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.

Adjust system clock automatically for daylight saving time.

Enable customized daylight saving time table.

APPLY

Customized Daylight Saving Time Tables

Add Daylight Saving Time Data

<input type="checkbox"/>	Start Time	End Time	Offset	Action
<input type="button" value="Delete"/>				

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.

The screenshot shows the 'General Settings' interface with the 'LANGUAGE' tab selected. Under the 'Language' section, there is a 'Filename Encoding' dropdown menu currently set to 'English'. An 'APPLY' button is located at the bottom right of the settings area.

Password Strength

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

The screenshot shows the 'General Settings' interface with the 'PASSWORD STRENGTH' tab selected. Under the 'Password Strength' section, there are three checkboxes, all of which are currently unchecked:

- 1. Please select a new password that contains characters from at least three of the following classes: lowercase letters, upper case letters, digits, and special characters.
- 2. No character in the new password may be repeated more than three times consecutively.
- 3. The new password must not be the same as the associated username, or the username reversed.

An 'APPLY' button is located at the bottom right of the settings area.

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.

Network

TCP/IP | WI-FI | DDNS | IPV6 | PROXY

IP Address

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC address	Speed	MTU	Link	Edit
Ethernet 1	No	10.8.13.59	255.255.254.0	10.8.12.1	00:08:9B:C5:A3:01	1000Mbps	1500		

Default Gateway

Use the settings from: Ethernet 1

DNS Server

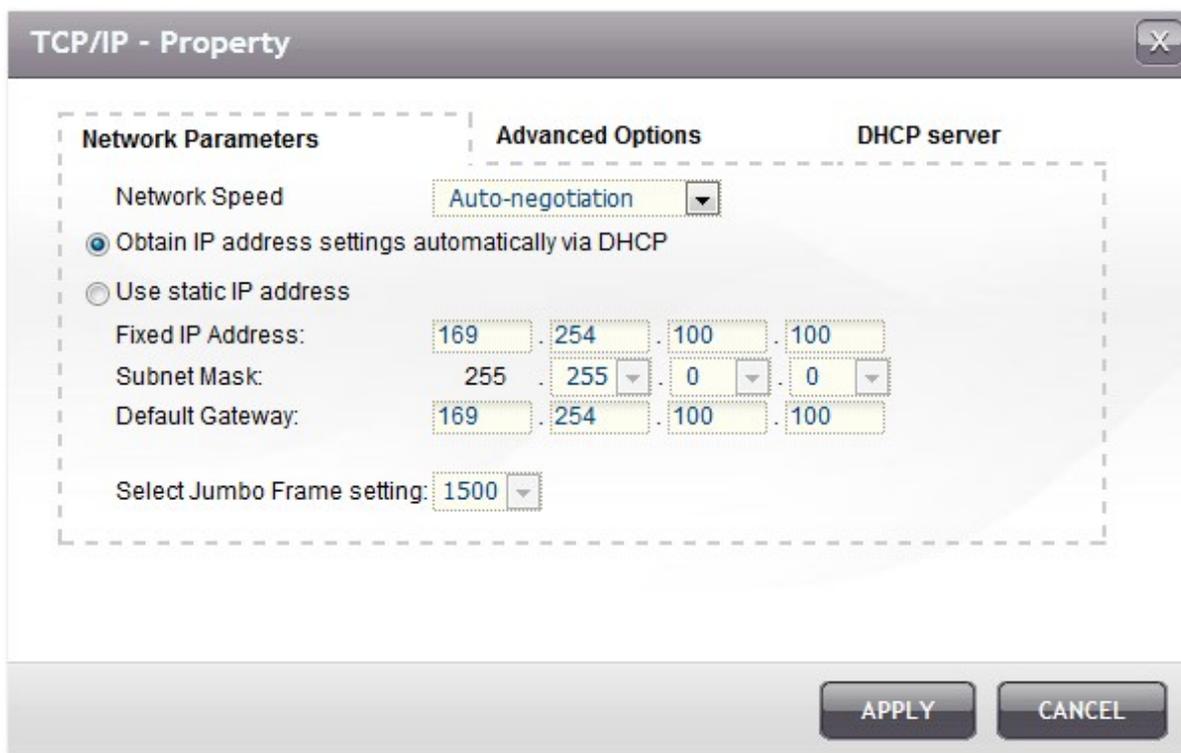
Obtain DNS server address automatically

Use the following DNS server address:

Primary DNS server: . . .

Secondary DNS server: . . .

APPLY



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 X

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

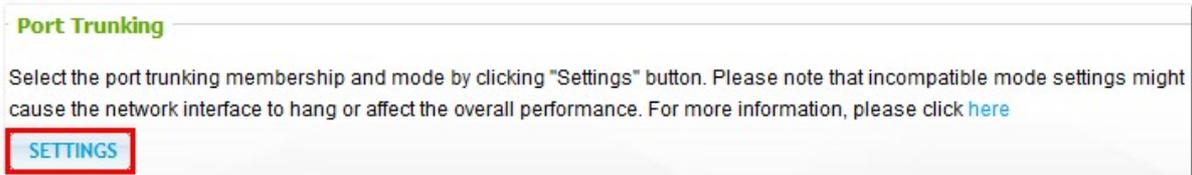
Applicable to NAS models with two or more LAN ports only.

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.

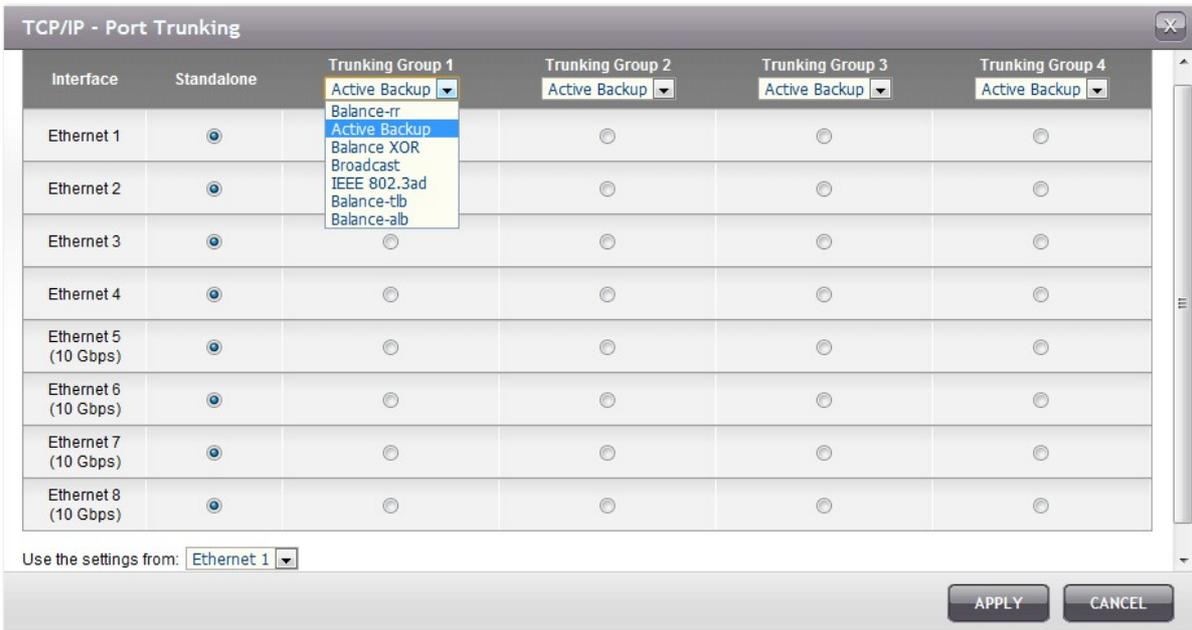
To use port trunking on the NAS, make sure at least two LAN ports of the NAS have been connected to the same switch and the settings described in sections (i) and (ii) have been configured.

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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 5 (10 Gbps)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 6 (10 Gbps)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 7 (10 Gbps)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethernet 8 (10 Gbps)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

IP Address										
Interface	VLAN (Virtual LAN)	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1+2	None	Yes	10.8.12.72	255.255.254.0	10.8.12.1	00:08:9B:C3:C7:D6	1000Mbps	1500		

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

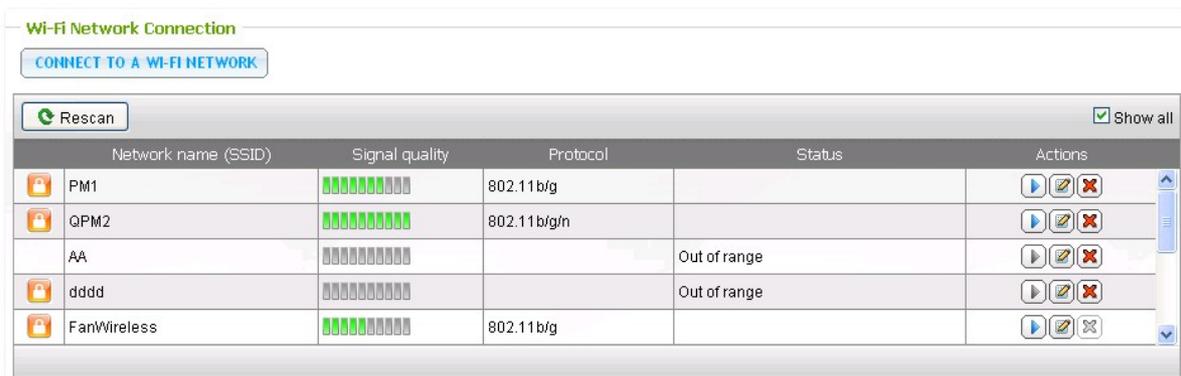
To connect the NAS to a Wi-Fi network, plug in a wireless dongle into a USB port of the NAS. The NAS will detect a list of wireless access points. You can connect the NAS to the Wi-Fi network in two ways.

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.



The screenshot shows the "Wi-Fi Network Connection" interface. At the top, there is a "CONNECT TO A WI-FI NETWORK" button and a "Rescan" button. A "Show all" checkbox is checked. Below is a table with the following data:

Network name (SSID)	Signal quality	Protocol	Status	Actions
PM1	██████████	802.11b/g		[Connect] [Edit] [Close]
QPM2	██████████	802.11b/g/n		[Connect] [Edit] [Close]
AA	██████████		Out of range	[Connect] [Edit] [Close]
dddd	██████████		Out of range	[Connect] [Edit] [Close]
FanWireless	██████████	802.11b/g		[Connect] [Edit] [Close]

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.



Rescan						Show all
Network name (SSID)	Signal quality	Protocol	Status	Actions		
QPM2	██████████	802.11b/g/n	Connecting	⏏	✎	✖
PM1	██████████	802.11b/g		▶	✎	✖
AA	██████████		Out of range	▶	✎	✖

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".



The screenshot shows a configuration window with two sections. The first section, titled "IP Address", contains a table with the following data:

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
WLAN 1	Yes	0.0.0.0	0.0.0.0	0.0.0.0	00:1F:1F:55:4E:3C	--	0		

The second section, titled "Wi-Fi Network Connection", contains a single button labeled "CONNECT TO A WI-FI NETWORK" which is highlighted with a red rectangular border.

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.

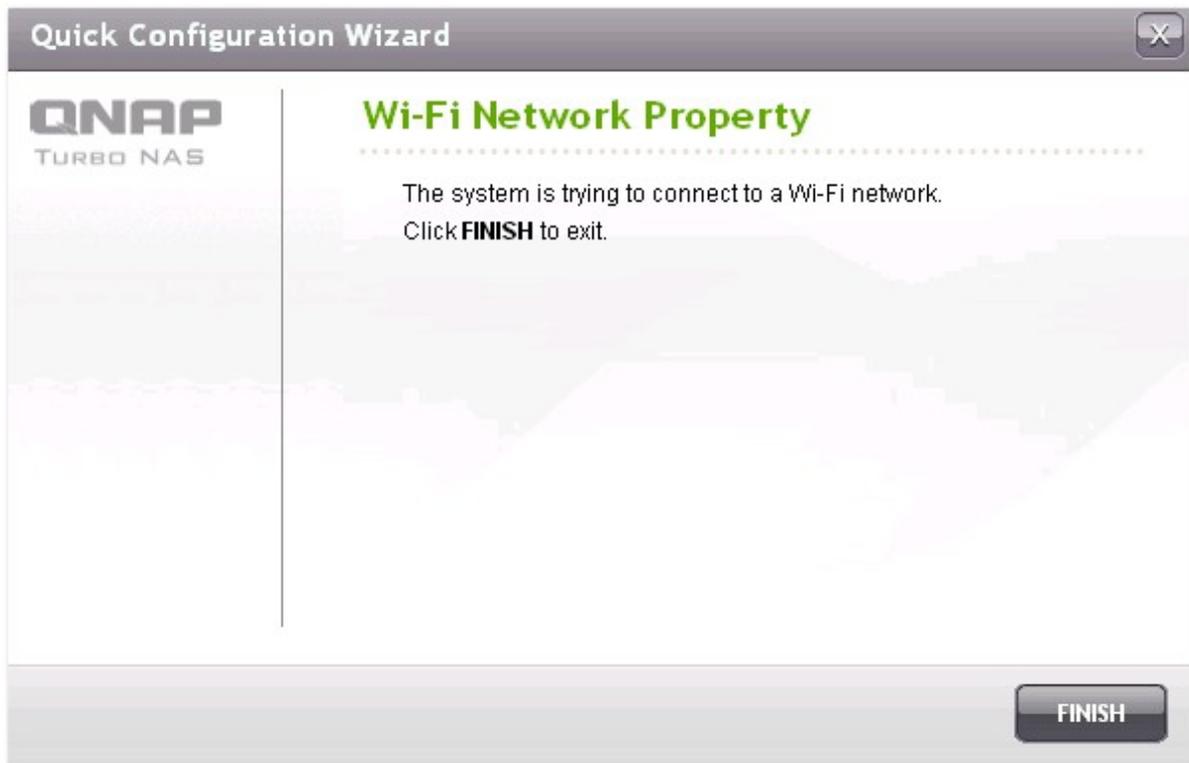
- No authentication (Open): No security key required.
- WEP: Enter up to 4 WEP keys and choose 1 key to be used for authentication.
- WPA-Personal: Choose either the AES or TKIP encryption type and enter the encryption key.
- WPA2-Personal: Enter a security key.

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.

IP Address									
Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
WLAN 1	Yes	192.168.11.6	255.255.255.0	0.0.0.0	00:1F:1F:55:4E:3C	54Mbps	1500		

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.

Network

TCP/IP | WI-FI | DDNS | IPV6 | PROXY

IP Address

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1	No	10.8.13.59	255.255.254.0	10.8.12.1	00:08:9B:C5:A3:01	1000Mbps	1500		

Default Gateway

Use the settings from:

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 here⁶⁷⁹.

Network

TCP/IP WI-FI **DDNS** IPV6 PROXY

DDNS Service

After enabling DDNS Service, you can connect to this server by domain name.

Enable Dynamic DNS Service

Select DDNS server:

Enter the account information you registered with the DDNS provider

Username:

Password:

Host name:

Check the external IP address automatically

Current WAN IP: 61.62.220.74

Recent DDNS Update Result

Connection IP last checked:

Next check for connection IP:

Last DDNS update time:

Update server response:

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)

Network

TCP/IP WI-FI DDNS **IPv6** PROXY

IP Address

Enable IPv6

Interface	Auto Configuration	IPv6 Address	Prefix Length	Gateway	Link	Edit
Ethernet 1	Yes	fe80::208:9bff:fe8c:bc6c	64	::		

DNS Server

::

::

APPLY

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 "::".

Proxy

Enter the proxy server settings to allow the NAS to access the Internet through a proxy server for live update of the firmware, virus definition update, and QPKG add-ons download.

Network

TCP/IP WI-FI DDNS IPV6 **PROXY**

Proxy

Use a proxy server

Proxy server:

Port:

Authentication

Username:

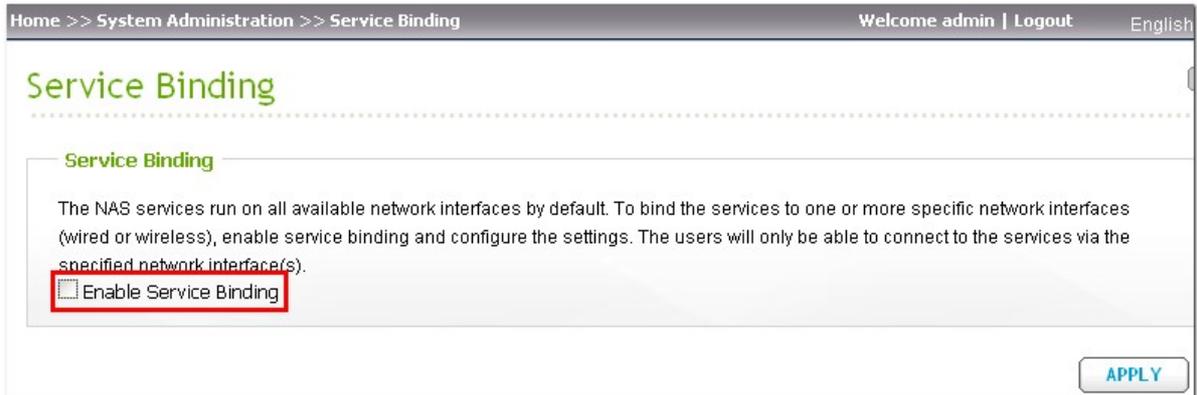
Password:

APPLY

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 screenshot shows a web interface for configuring Service Binding. The breadcrumb navigation at the top reads "Home >> System Administration >> Service Binding". On the right side of the header, it says "Welcome admin | Logout" and "English". The main heading is "Service Binding". Below the heading, there is a section titled "Service Binding" with a sub-heading. The text in this section reads: "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 and configure the settings. The users will only be able to connect to the services via the specified network interface(s)." Below this text is a checkbox labeled "Enable Service Binding", which is currently unchecked and highlighted with a red box. At the bottom right of the form, there is an "APPLY" button.

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.

Enable Service Binding

	Ethernet 1	Ethernet 2
Network Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apple Networking ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NFS Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
iSCSI Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Management Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NAS Web Management Interface ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SSH Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Telnet Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application Servers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web Server ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MySQL Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RTRR Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Rsync Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3.4 Hardware

Configure the hardware functions of the NAS.

Hardware

- Enable configuration reset switch
- Enable hard disk standby mode if no access within the specific time period : 30 minutes ?
- Enable light signal alert when the free size of disk is less than the value: 3072 MB
- Enable write cache (EXT4 only)

Buzzer Control

Enable alarm buzzer

- System operations (startup, shutdown, and firmware upgrade)
- System events (error and warning)

Smart Fan Configuration

Fan Rotation Speed Settings: Enable Smart Fan (recommended) ▼

- When ALL of the following temperature readings are met the fan will rotate at low speed:
 - The system temperature is lower than 40°C(104°F).
- When ANY of the following temperature readings are met the fan will rotate at high speed:
 - The system temperature is higher than or equal to 57°C(135°F).
 - The CPU temperature is higher than or equal to 62°C(144°F).
- Self-defined temperature:
 - When the system temperature is lower than 25 °C , stop fan rotation.
 - When the system temperature is lower than 35 °C , rotate at low speed.
 - When the system temperature is higher than 45 °C , rotate at high speed.

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.

Security

- SECURITY LEVEL
- NETWORK ACCESS PROTECTION
- SSL SECURE CERTIFICATE & PRIVATE KEY

Security Level

High: Allow connections from the list only

Medium: Deny connections from the list

Low: Allow all connections

Enter the IP address or network from which the connections to this server will be allowed or rejected.

+ -

Genre	IP address or network domain	Time left for IP blocking
-------	------------------------------	---------------------------

APPLY

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.

Security

SECURITY LEVEL **NETWORK ACCESS PROTECTION** **SSL SECURE CERTIFICATE & PRIVATE KEY**

Network Access Protection

Enable network access protection

<input checked="" type="checkbox"/> SSH:	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes
<input checked="" type="checkbox"/> Telnet:	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes
<input checked="" type="checkbox"/> HTTP(S):	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes
<input type="checkbox"/> FTP:	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes
<input type="checkbox"/> SAMBA:	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes
<input type="checkbox"/> AFP:	In	1 minutes	, after unsuccessful attempts for	5 time(s)	, block the IP for	5 minutes

APPLY

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.

Security

SECURITY LEVEL **NETWORK ACCESS PROTECTION** **SSL SECURE CERTIFICATE & PRIVATE KEY**

SSL Secure Certificate & Private Key

You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate successfully, you can access the administration interface by SSL connection and there will not be any alert or error message.

If you upload an incorrect secure certificate, you may not be able to login the server via SSL. To resolve the problem, you can restore the secure certificate to default and access the system again.

Status: Uploaded secure certificate being used

Certificate: Please enter a certificate in X.509PEM format below.

Private Key: Please enter a certificate or private key in X.509PEM format below.

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.

The screenshot shows a web browser window with the following elements:

- Header: Home >> System Administration >> Notification | Welcome admin | Logout | English
- Section: Notification
- Navigation: CONFIGURE SMTP SERVER (active), CONFIGURE IM, CONFIGURE SMSC SERVER, ALERT NOTIFICATION
- Form Title: Configure SMTP Server
- Fields:
 - SMTP Server: [Redacted]
 - Port Number: 465
 - Sender: [Redacted]
 - Enable SMTP Authentication
 - User Name: [Redacted]
 - Password: [Redacted]
 - Use SSL/TLS secure connection
 - Protocol Type: SSL (dropdown)
- Button: APPLY

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".

Notification

CONFIGURE SMTP SERVER **CONFIGURE IM** CONFIGURE SMSC SERVER ALERT NOTIFICATION

Configure Instant Messaging Service

Enable Instant Messaging Service

Email: [Redacted]

Password: [Redacted]

Login Status: On

APPLY

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".

Notification

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

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.

Notification

CONFIGURE SMTP SERVERCONFIGURE IMCONFIGURE SMSC SERVERALERT NOTIFICATION

Configure SMSC Server

You can configure the SMSC settings to send instant system alerts via the SMS service provided by the SMS provider.

SMS Service Provider: Clickatell ▼ <http://www.clickatell.com>

Enable SSL Connection

SSL Port: 443

SMS Server Login Name:

SMS Server Login Password:

SMS Server API_ID:

APPLY

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: [v](#)

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.

Power Management

Restart/ Shutdown

Execute system restart/ shutdown immediately.

EuP Mode Configuration

Enable
 Disable

Configure Wake on LAN

Enable
 Disable

When the AC power resumes

Resume the server to the previous power-on or power-off status.
 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	▼	17	▼	2	▼	+	-
Shutdown	▼	Daily	▼	17	▼	5	▼	+	-

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".

The screenshot shows a web interface for configuring the Network Recycle Bin. The title is "Network Recycle Bin" in green. Below the title, there is a section titled "Network Recycle Bin" with a dashed line separator. The text reads: "After enabling Network Recycle Bin, all the deleted files on the network folders of the NAS are moved to the 'Network Recycle Bin' network folder." There are three checked checkboxes: "Enable Network Recycle Bin", "File retention time : 180 day(s)", and "Exclude these file extensions: (case insensitive, separated by comma ',')". Below the last checkbox is a text input field containing "tmp, temp, wtmp, blk, dat". Below this section is another section titled "Empty Network Recycle Bin" with a dashed line separator. The text reads: "Click [EMPTY NETWORK RECYCLE BIN] to delete all the files in network recycle bin." There is a button labeled "EMPTY NETWORK RECYCLE BIN" and an "APPLY" button at the bottom right of the interface.

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".

Back up/Restore Settings

Back up System Settings

To backup all settings, including user accounts, server name and network configuration etc., click **[BACK UP]** and select to open or save the setting file.

Restore System Settings

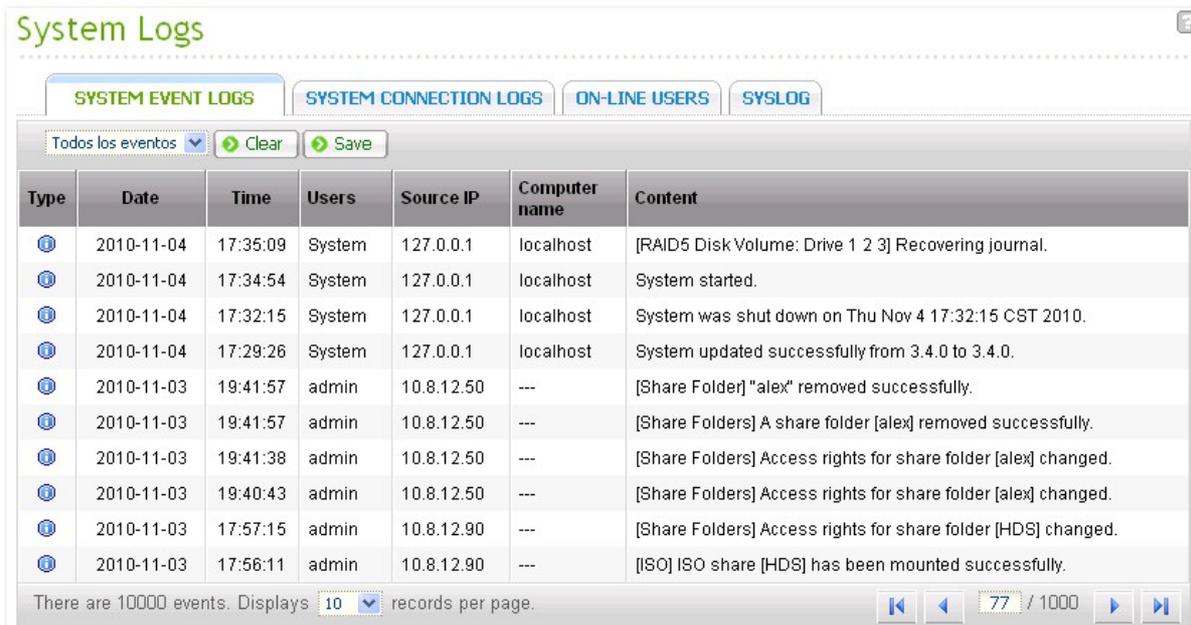
To restore all settings, click **[Browse...]** to select a previously saved setting file and click **[RESTORE]** to confirm.

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".



The screenshot shows a web interface titled "System Logs" with a tab for "SYSTEM EVENT LOGS". Below the tabs are buttons for "Clear" and "Save", and a dropdown menu set to "Todos los eventos". The main area contains a table with the following columns: Type, Date, Time, Users, Source IP, Computer name, and Content. The table lists 10 events from 2010-11-03 to 2010-11-04. At the bottom, it indicates "There are 10000 events. Displays 10 records per page." and includes navigation controls for page 77 of 1000.

Type	Date	Time	Users	Source IP	Computer name	Content
①	2010-11-04	17:35:09	System	127.0.0.1	localhost	[RAID5 Disk Volume: Drive 1 2 3] Recovering journal.
①	2010-11-04	17:34:54	System	127.0.0.1	localhost	System started.
①	2010-11-04	17:32:15	System	127.0.0.1	localhost	System was shut down on Thu Nov 4 17:32:15 CST 2010.
①	2010-11-04	17:29:26	System	127.0.0.1	localhost	System updated successfully from 3.4.0 to 3.4.0.
①	2010-11-03	19:41:57	admin	10.8.12.50	---	[Share Folder] "alex" removed successfully.
①	2010-11-03	19:41:57	admin	10.8.12.50	---	[Share Folders] A share folder [alex] removed successfully.
①	2010-11-03	19:41:38	admin	10.8.12.50	---	[Share Folders] Access rights for share folder [alex] changed.
①	2010-11-03	19:40:43	admin	10.8.12.50	---	[Share Folders] Access rights for share folder [alex] changed.
①	2010-11-03	17:57:15	admin	10.8.12.90	---	[Share Folders] Access rights for share folder [HDS] changed.
①	2010-11-03	17:56:11	admin	10.8.12.90	---	[ISO] ISO share [HDS] has been mounted successfully.

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".

System Logs

SYSTEM EVENT LOGS | **SYSTEM CONNECTION LOGS** | ON-LINE USERS | SYSLOG

Todos los eventos | Options | Stop logging | Clear | Save

Type	Date	Time	Users	Source IP	Computer name	Connection type	Accessed resources	Action
①	2010-12-28	15:57:43	admin	10.8.12.68	---	HTTP	Administration	Login OK
①	2010-12-28	14:59:58	admin	10.8.12.43	---	HTTP	Administration	Login OK
①	2010-12-28	14:54:43	admin	10.8.12.68	---	SSH	---	Login OK
①	2010-12-28	14:53:00	admin	10.8.12.68	---	HTTP	Administration	Login OK
①	2010-12-28	14:22:23	admin	10.8.12.43	---	HTTP	Administration	Login OK
①	2010-12-28	12:39:24	admin	10.8.12.43	---	HTTP	Administration	Login OK
①	2010-12-28	10:56:12	admin	10.8.12.43	---	HTTP	Administration	Login OK
①	2010-12-27	06:50:29	admin	10.8.12.43	---	HTTP	Administration	Login OK
①	2010-12-27	03:37:26	admin	10.8.12.51	---	HTTP	Administration	Login OK
①	2010-12-27	10:24:19	admin	10.8.12.43	---	HTTP	Administration	Login OK

There are 994 events. Displays 10 records per page. 1 / 100

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.

Connection Type

Select the connection type to be logged.

HTTP FTP Telnet SSH
 AFP SAMBA iSCSI

When the number of logs reaches 10,000, archive the connection logs and save the file in the folder:

APPLY CANCEL

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".

SYSTEM EVENT LOGS **SYSTEM CONNECTION LOGS** ON-LINE USERS SYSLOG

All events Options Stop logging Clear Save

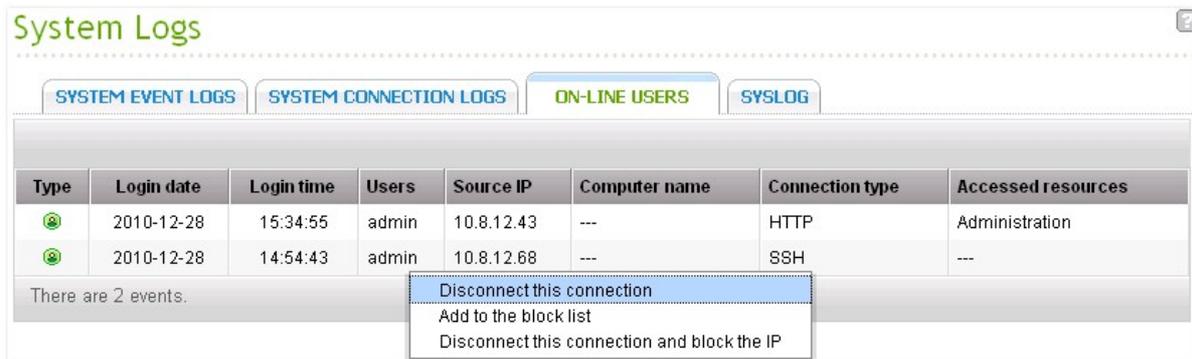
Type	Date	Time	Users	Source IP	Computer name	Connectic type	Accessed resources	Action
ⓘ	2011-01-19	08:55:28	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documen	Delete
ⓘ	2011-01-19	08:55:26	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documen	Read
ⓘ	2011-01-19	08:55:21	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documen	Read
ⓘ	2011-01-19	08:55:20	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documen	Read
ⓘ	2011-01-19	08:55:19	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documen	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 Documen	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

There are 10000 events. Displays records per page. 1 / 1000

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.



The screenshot shows a web interface titled "System Logs" with a navigation bar containing "SYSTEM EVENT LOGS", "SYSTEM CONNECTION LOGS", "ON-LINE USERS", and "SYSLOG". The "ON-LINE USERS" tab is active. Below the navigation bar is a table with the following columns: Type, Login date, Login time, Users, Source IP, Computer name, Connection type, and Accessed resources. The table contains two rows of data. A context menu is open over the second row, showing three options: "Disconnect this connection", "Add to the block list", and "Disconnect this connection and block the IP".

Type	Login date	Login time	Users	Source IP	Computer name	Connection type	Accessed resources
	2010-12-28	15:34:55	admin	10.8.12.43	---	HTTP	Administration
	2010-12-28	14:54:43	admin	10.8.12.68	---	SSH	---

There are 2 events.

- Disconnect this connection
- Add to the block list
- Disconnect this 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.

System Logs

SYSTEM EVENT LOGS
SYSTEM CONNECTION LOGS
ON-LINE USERS
SYSLOG

Syslog Settings

Enable syslog
 You can enable this option to save the event logs and connection logs to a remote syslog server.

Syslog Server IP:

UDP Port:

Select the logs to record

System Event Logs

System Connection Logs (You must enable system connection logs to use this option.)

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

Firmware Update

FIRMWARE UPDATE **LIVE UPDATE**

Firmware Update

Current firmware version: 3.8.0 Build 20121114

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

1. Download the release notes of the same version as the firmware from QNAP website <http://www.qnap.com/>. Read the release notes carefully to make sure you need to update the firmware.
2. Before updating system firmware, back up all disk data on the server to avoid any potential data loss during system update.
3. Click the **[Browse...]** button to select the correct firmware image for system update. Click the **[Update System]** button to update the firmware.

Browse...

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

UPDATE SYSTEM

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

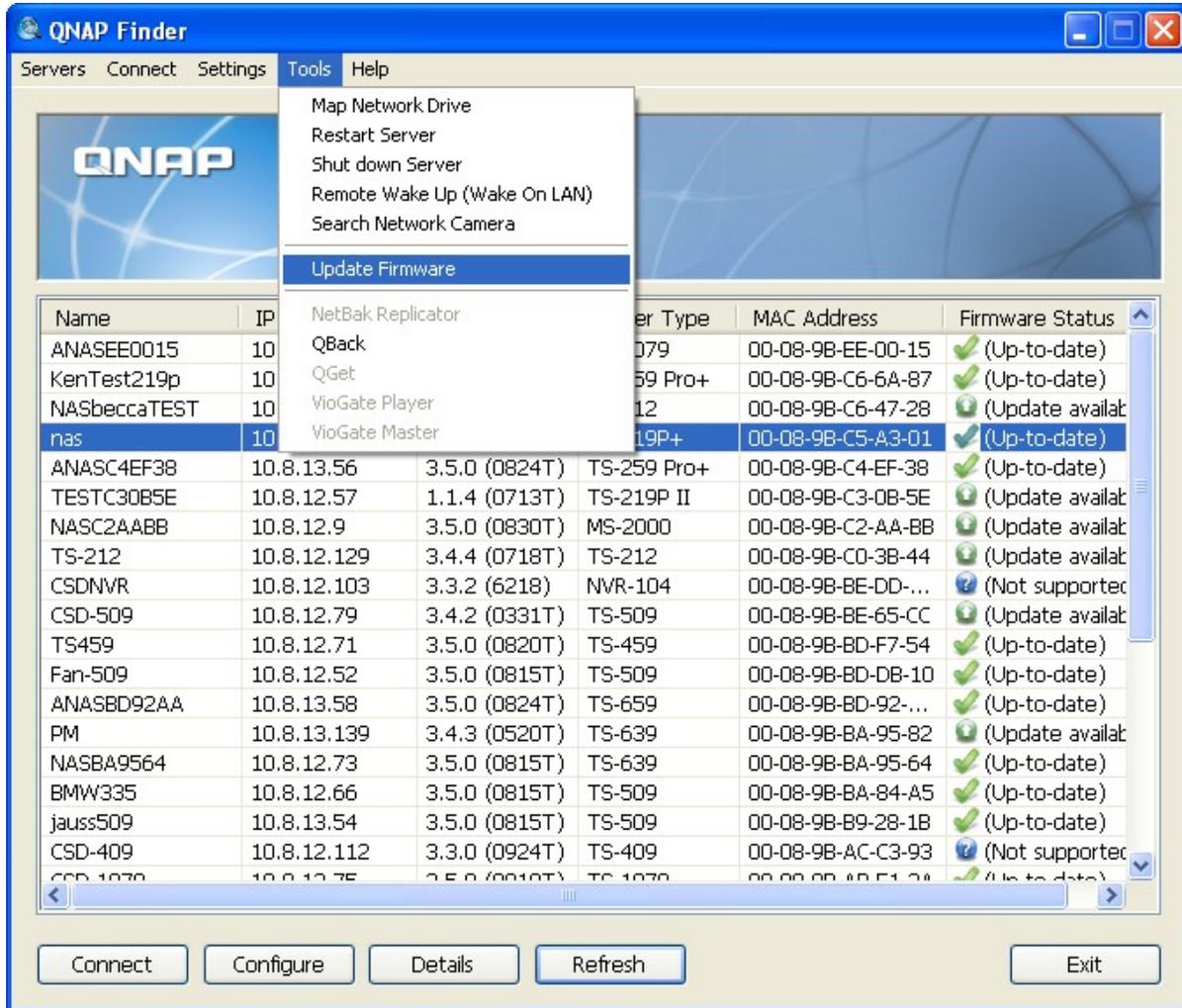
Before updating the system firmware, make sure the product model and firmware version are correct. Follow the steps below to update firmware:

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.

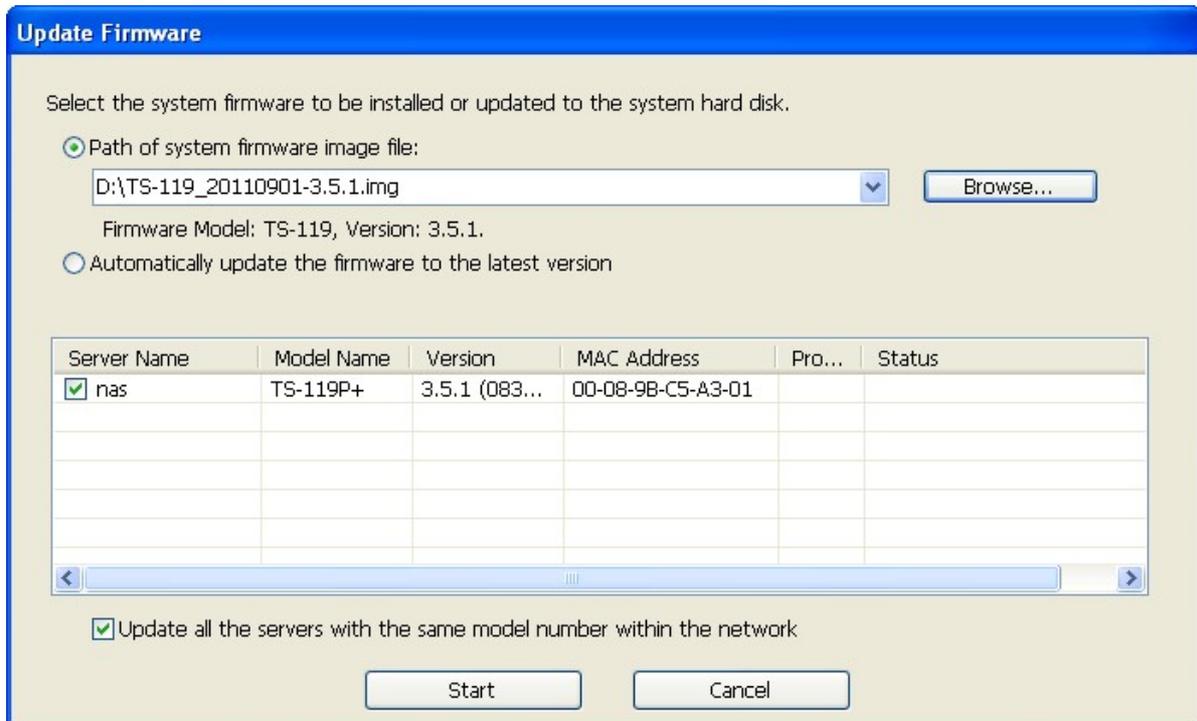


Login the NAS as an administrator.



The dialog box titled "Login Administrator [nas]" has a blue header bar with a close button (X) in the top right corner. It contains two text input fields: "Administrator Name" with the text "admin" and "Administrator Password" with seven dots. Below the fields are two buttons: "OK" and "Cancel".

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



The dialog box titled "Update Firmware" has a blue header bar. Below the header, it says "Select the system firmware to be installed or updated to the system hard disk." There are two radio buttons: "Path of system firmware image file:" (selected) and "Automatically update the firmware to the latest version". The selected option has a text box containing "D:\TS-119_20110901-3.5.1.img" and a "Browse..." button. Below this, it says "Firmware Model: TS-119, Version: 3.5.1." Below the radio buttons is a table with the following data:

Server Name	Model Name	Version	MAC Address	Pro...	Status
<input checked="" type="checkbox"/> nas	TS-119P+	3.5.1 (083...	00-08-9B-C5-A3-01		

Below the table is a horizontal scrollbar. At the bottom, there is a checked checkbox "Update all the servers with the same model number within the network" and two buttons: "Start" and "Cancel".

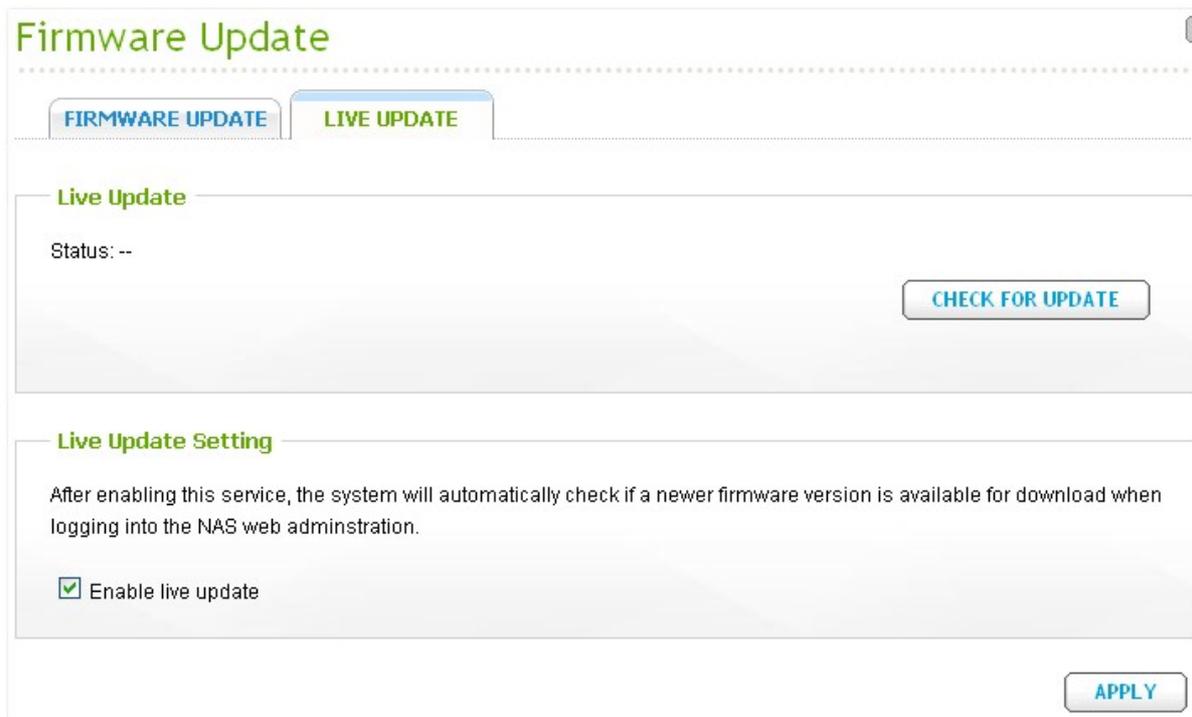
Note: The NAS servers of the same model on the same LAN can be updated by the Finder at the same time. Administrator access is required for system update.

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.



The screenshot displays the 'Firmware Update' configuration page. At the top, there are two tabs: 'FIRMWARE UPDATE' and 'LIVE UPDATE', with the latter being the active tab. Below the tabs, the 'Live Update' section shows a 'Status: --' and a 'CHECK FOR UPDATE' button. The 'Live Update Setting' section contains a descriptive paragraph and a checked checkbox for 'Enable live update'. An 'APPLY' button is located at the bottom right of the page.

Firmware Update

FIRMWARE UPDATE **LIVE UPDATE**

Live Update

Status: --

[CHECK FOR UPDATE](#)

Live Update Setting

After enabling this service, the system will automatically check if a newer firmware version is available for download when logging into the NAS web administration.

Enable live update

[APPLY](#)

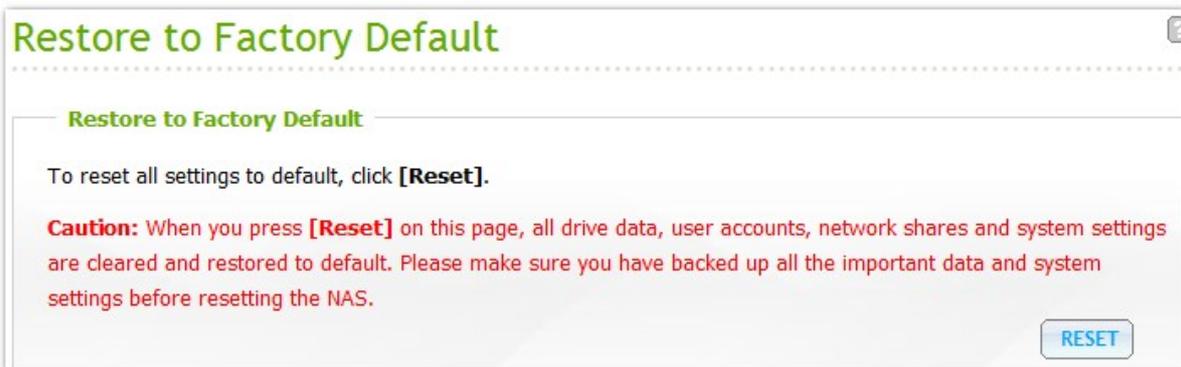
3.12 Restore to Factory Default

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"[\[64\]](#).



4. Disk Management

[Volume Management](#)^[92]

[RAID Management](#)^[96]

[Hard Disk SMART](#)^[122]

[Encrypted File System](#)^[123]

[iSCSI](#)^[132]

[Virtual Disk](#)^[192]

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.

Volume Management



Single Disk Volume
Create single disk volume(s).



RAID 1 Mirroring Disk Volume
Create mirroring disk volume(s).



RAID 0 Striping Disk Volume
Create one striping disk volume.



RAID 10 Disk Volume
Combine an even number of disks (minimum 4 disks) to create a disk volume with data protection.



JBOD Linear Disk Volume
Create one linear disk volume.



RAID 5 Disk Volume
Combine 3 or more disks to create a disk volume with data protection (1 failed disk is allowed).



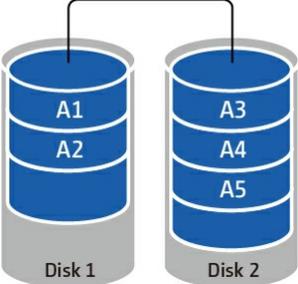
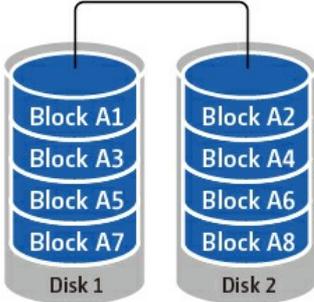
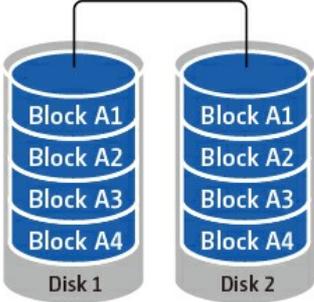
RAID 6 Disk Volume
Combine 4 or more disks to create a disk volume with data protection (2 failed disks are allowed).

Current Disk Volume Configuration : Physical Disks

Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	Hitachi HDT725032VLA360 V540	298.09 GB	Ready	SCAN NOW	GOOD
Drive 2	Seagate ST3250620AS 3.AA	232.89 GB	Ready	SCAN NOW	GOOD
Drive 3	Seagate ST3250620AS 3.AA	232.89 GB	Ready	SCAN NOW	GOOD
Drive 4	--	--	No Disk	SCAN NOW	---
Drive 5	--	--	No Disk	SCAN NOW	---

Note that if you are going to 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.

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

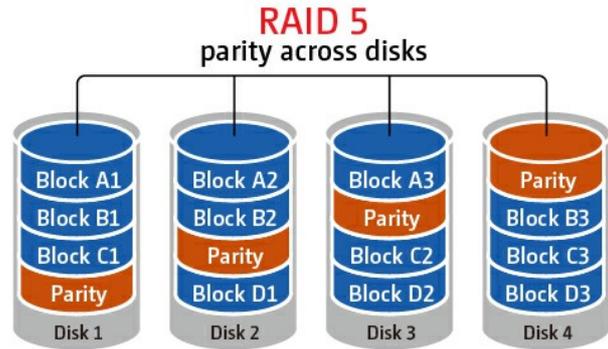
<p>Single Disk Volume</p> <p>Each hard drive is used as a standalone disk. If a hard drive is damaged, all the data will be lost.</p>	
<p>JBOD (Just a bunch of disks)</p> <p>JBOD is a collection of hard drives that does not offer any RAID protection. The data are written to the physical disks sequentially. The total storage capacity is equal to the sum of the capacity of all member hard drives.</p>	<p style="text-align: center;">JBOD</p> 
<p>RAID 0 Striping Disk Volume</p> <p>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.</p>	<p style="text-align: center;">RAID 0 striping</p> 
<p>RAID 1 Mirroring Disk Volume</p> <p>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.</p>	<p style="text-align: center;">RAID 1 mirroring</p> 

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.

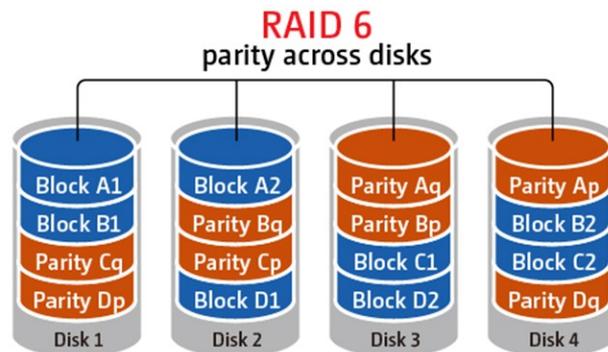
The storage capacity of a RAID 5 array is equal to $(N-1) * (\text{size of smallest hard drive})$. N is the number of hard drives in the array.



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.

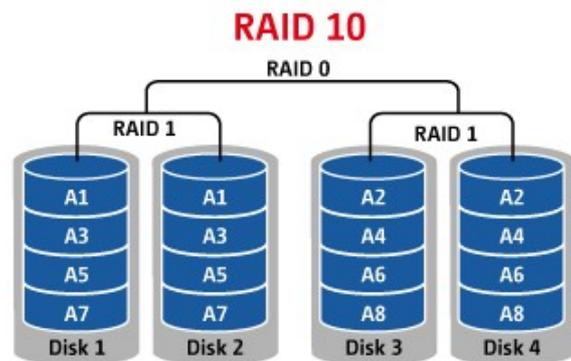
To create a RAID 6 disk volume, a minimum of 4 hard drives are required. The storage capacity of a RAID 6 array is equal to $(N-2) * (\text{size of smallest hard drive})$. N is the number of hard drives in the array.



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 $(\text{size of the smallest capacity disk in the array}) * N/2$. 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.

RAID Management ?

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration

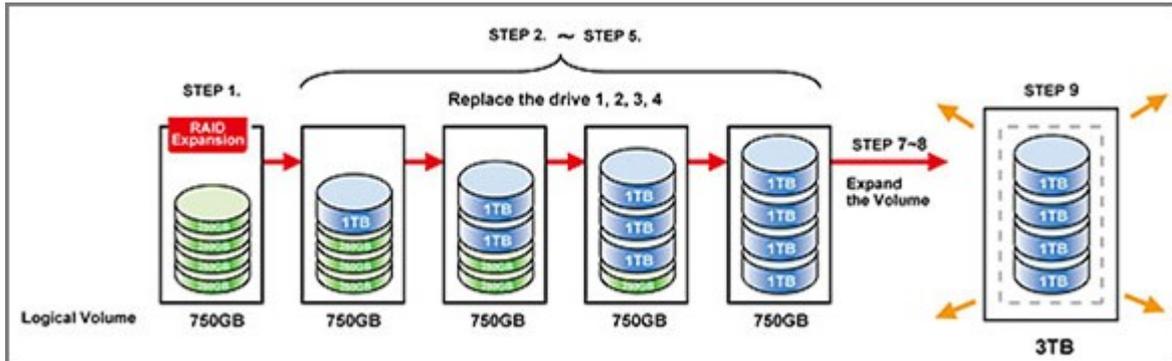
Volume	Total Size	Bitmap	Status	Description
<input type="radio"/> Mirroring Disk Volume: Drive 1 2	145.24 GB	No	Ready	The operation(s) you can execute: - Expand capacity

Expand Capacity (Online RAID Capacity Expansion)

Scenario

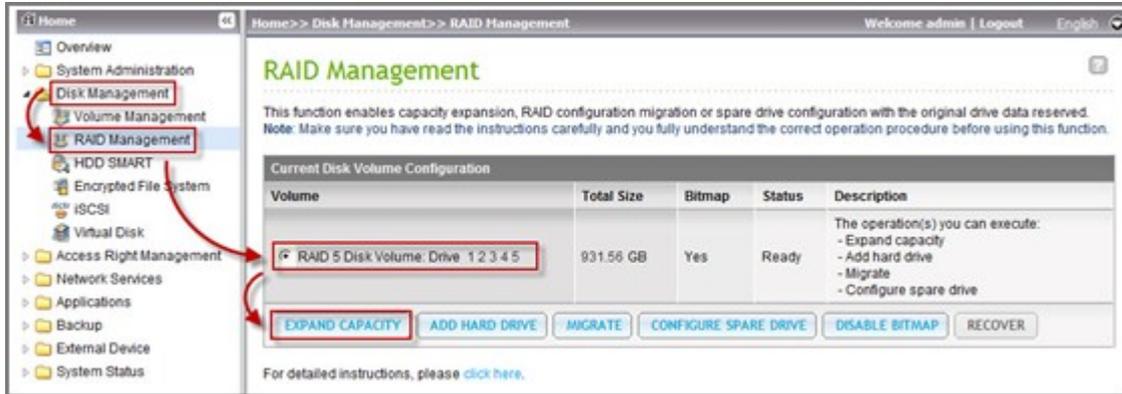
You bought four 250GB hard drives for initial setup of a TS-509 Pro NAS and configured RAID 5 disk configuration with the four hard drives.

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.

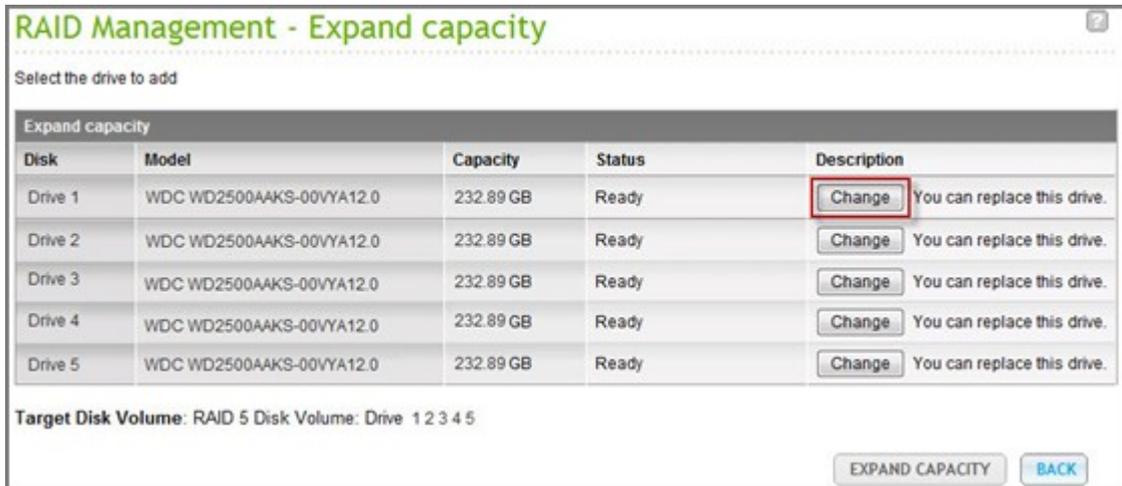


Operation procedure

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.

RAID Management - Expand capacity ?

Select the drive to add

Expand capacity				
Disk	Model	Capacity	Status	Description
Drive 1	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	<input type="button" value="Cancel"/> <input type="button" value="Please remove the drive"/>
Drive 2	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 3	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 4	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 5	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy

Target Disk Volume: RAID 5 Disk Volume: Drive 1 2 3 4 5

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

RAID Management - Expand capacity ?

Select the drive to add

Expand capacity				
Disk	Model	Capacity	Status	Description
Drive 1	--	--	No Disk	<input type="button" value="Please insert the new drive"/>
Drive 2	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 3	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 4	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy
Drive 5	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	No operation can be executed on this drive or the drive is busy

Target Disk Volume: RAID 5 Disk Volume: Drive 2 3 4 5

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.

RAID Management - Expand capacity ?

Select the drive to add

Expand capacity				
Disk	Model	Capacity	Status	Description
Drive 1	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	<input type="button" value="Change"/> You can replace this drive.
Drive 2	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	<input type="button" value="Change"/> You can replace this drive.
Drive 3	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	<input type="button" value="Change"/> You can replace this drive.
Drive 4	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	<input type="button" value="Change"/> You can replace this drive.
Drive 5	WDC WD2500AAKS-00VYA12.0	232.89 GB	Ready	<input type="button" value="Change"/> You can replace this drive.

Target Disk Volume: RAID 5 Disk Volume: Drive 1 2 3 4 5

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

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration

Volume	Total Size	Bitmap	Status	Description
RAID 5 Disk Volume: Drive 1 2 3 4 5	913.96 GB	Yes	Ready	The operation(s) you can execute: - Expand capacity

EXPAND CAPACITY ADD HARD DRIVE MIGRATE CONFIGURE SPARE DRIVE BITMAP RECOVER

For detailed instructions, please [click here](#).

Click "OK" to proceed.

The NAS beeps and starts to expand the capacity.

RAID Management - Expand capacity

Select the drive to add

Expand capacity

Disk	Model	Capacity	Status	Description
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	Processing...
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	Processing...
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	Processing...
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	Processing...
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	Processing...

Target Disk Volume: RAID 5 Disk Volume: Drive 1 2 3 4 5 You can expand the disk volume capacity to approximately **3726 GB**

EXPAND CAPACITY BACK

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.)

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration				
Volume	Total Size	Bitmap	Status	Description
<input checked="" type="radio"/> RAID 5 Disk Volume: Drive 1 2 3 4 5	3726.04 GB	Yes	Ready	The operation(s) you can execute: - Expand capacity

EXPAND CAPACITY
ADD HARD DRIVE
MIGRATE
CONFIGURE SPARE DRIVE
BITMAP
RECOVER

For detailed instructions, please [click here](#).

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)

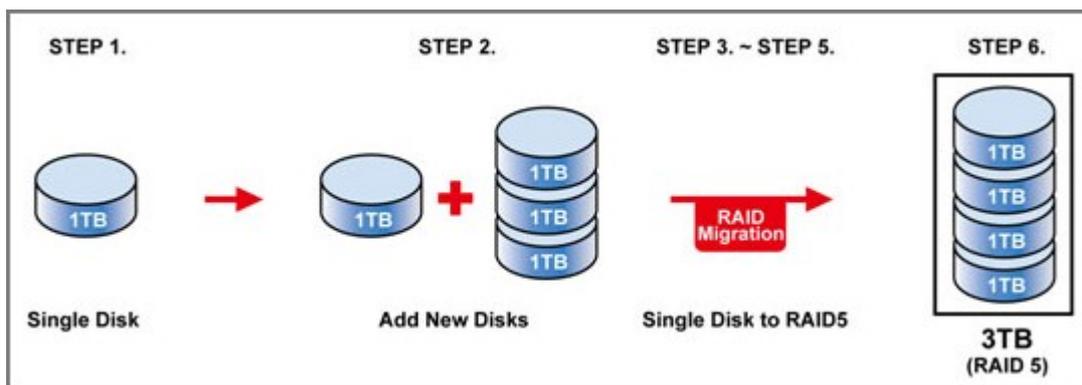
During the initial setup of the TS-509 Pro, you bought a 1TB hard drive and configured it as single disk. The TS-509 Pro is used as a file server for data sharing among the departments.

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).

Current Disk Volume Configuration: Physical Disks					
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	--	--	No Disk	SCAN NOW	---
Drive 3	--	--	No Disk	SCAN NOW	---
Drive 4	--	--	No Disk	SCAN NOW	---
Drive 5	--	--	No Disk	SCAN NOW	---

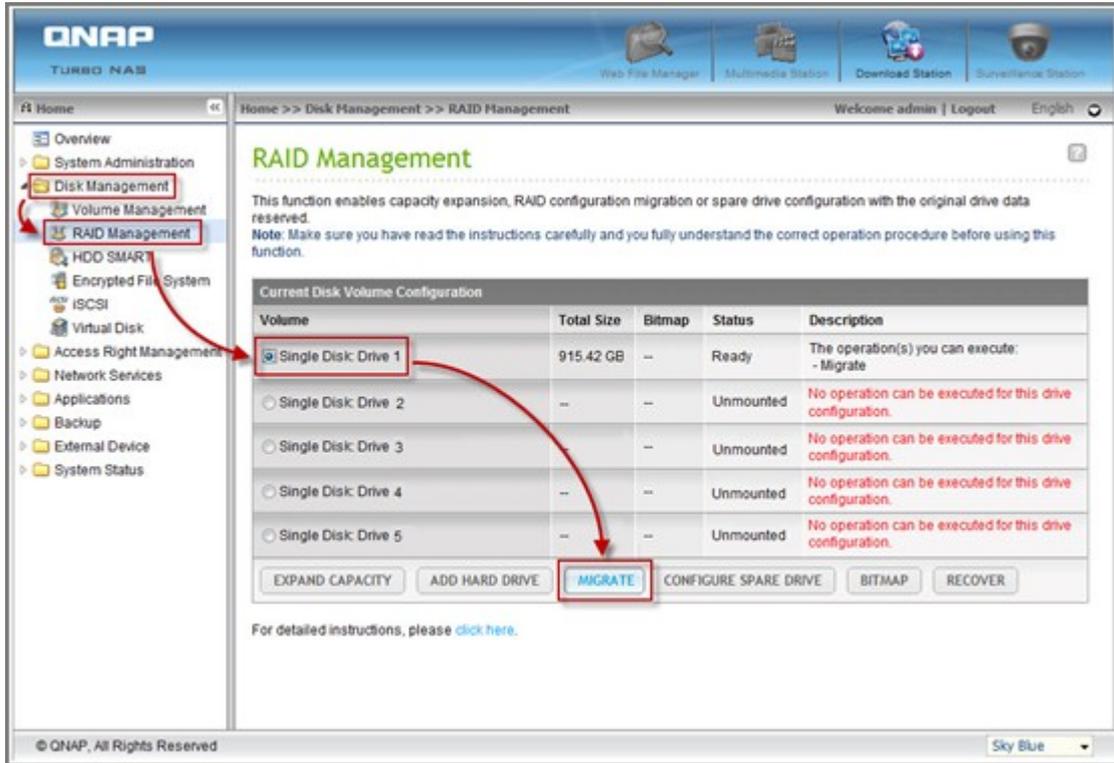
Current Disk Volume Configuration: Logical Volumes				
Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 1	EXT3	931.51 GB	524.68 GB	Ready
FORMAT NOW CHECK NOW REMOVE NOW				

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 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKA0	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".

RAID Management - Migrate

Select the drive to add

Migrate				
Available drive(s)	Disk	Model	Capacity	Status
<input checked="" type="checkbox"/>	Drive 2	WD1000FYPS-01ZKB02.0	931.51 GB	Ready
<input checked="" type="checkbox"/>	Drive 3	WD1000FYPS-01ZKB02.0	931.51 GB	Ready
<input checked="" type="checkbox"/>	Drive 4	WD1000FYPS-01ZKB02.0	931.51 GB	Ready
<input checked="" type="checkbox"/>	Drive 5	WD1000FYPS-01ZKB02.0	931.51 GB	Ready

Select the migration method:

- Single Disk Volume -> RAID 1 Mirroring Disk Volume
- Single Disk Volume -> RAID 5 Disk Volume
- Single Disk Volume -> RAID 6 Disk Volume

Target Disk Volume: Single Disk: Drive 4 The drive configuration is about to be configured as RAID 5 Disk Volume, The capacity is approximately 3726 GB

MIGRATE **BACK**

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 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKA0	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.

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration				
Volume	Total Size	Bitmap	Status	Description
Single Disk: Drive 1	915.42 GB	--	Migrating... (2%)	No operation can be executed for this drive configuration

EXPAND CAPACITY ADD HARD DRIVE MIGRATE CONFIGURE SPARE DRIVE BITMAP RECOVER

For detailed instructions, please [click here](#).

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.

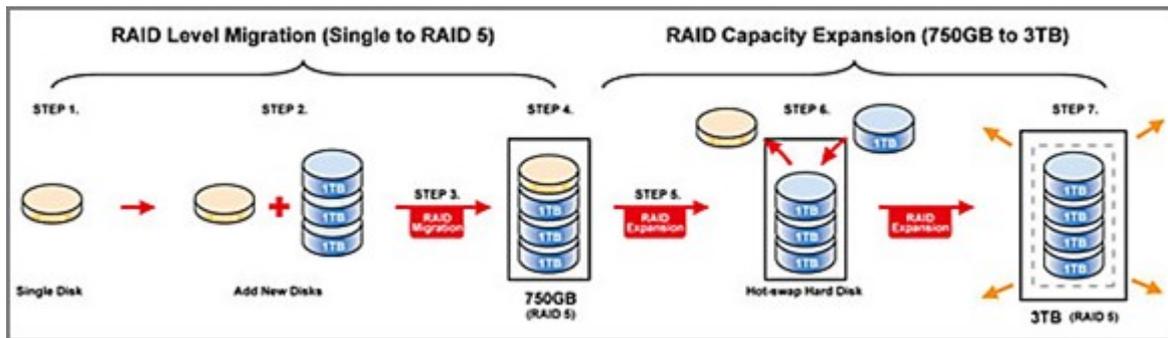
Use Online RAID Capacity Expansion and Online RAID Level Migration

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 $250\text{GB} \times 4$ 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 volume and click "ENABLE BITMAP".

Note: Bitmap support is only available for RAID 1, 5, 6, and 10.

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration

Volume	Total Size	Bitmap	Status	Description
RAID 5 Disk Volume: Drive 1 2 3	455.52 GB	No	Ready	The operation(s) you can execute: - Expand capacity

[EXPAND CAPACITY](#) [ADD HARD DRIVE](#) [MIGRATE](#) [CONFIGURE SPARE DRIVE](#) [ENABLE BITMAP](#) [RECOVER](#)

For detailed instructions, please [click here](#).

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 unplugged 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.

Current Disk Volume Configuration				
Disk/ Volume	Total Size	Bitmap	Status	Description
<input checked="" type="radio"/> Single Disk: Drive 6	--	--	Unmounted	The operation(s) you can execute: - Set global spare
<input type="radio"/> Mirroring Disk Volume: Drive 1 5	291.94 GB	No	Ready	The operation(s) you can execute: - Expand capacity - Migrate - Enable Bitmap

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".

Current Disk Volume Configuration				
Disk/ Volume	Total Size	Bitmap	Status	Description
<input checked="" type="radio"/> Single Disk: Drive 6	--	--	Global Spare	The operation(s) you can execute: - Cancel global spare
<input type="radio"/> Mirroring Disk Volume: Drive 1 5	291.94 GB	No	Ready	The operation(s) you can execute: - Expand capacity - Enable Bitmap

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.

HDD SMART

Monitor hard disk health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select Hard Disk: **Disk 1**

SUMMARY | HARD DISK INFORMATION | SMART INFORMATION | TEST | SETTINGS

Summary

Good

No errors were detected on the hard disk. Your hard disk should be operating properly.

Hard Disk Model	Hitachi Deskstar T7K500
Drive Capacity	298.09 GB
Hard Drive Health	Good
Hard Drive Temperature	44 °C
Test Time	---
Test Result	Not tested

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.



Volume	Total Size	Status	Action
Mirroring Disk Volume: Drive 1 2	145.24 GB	Unlocked	ENCRYPTION KEY MANAGEMENT

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.

Step 6

Step 6/6: Select the disk configuration

Note: All drive data will be cleared unless you select not to initialize the hard drives.

Please select the disk configuration for the initialization.

Disk configuration:

File System:

Total available storage capacity: 464.26 GB

You may select to use the hard drives as single disk volumes. However, when a drive failure occurs, all data will be lost.

Encrypt disk volume:

Input Encryption Password:

Verify Encryption Password:

Use Default Value Save Encryption Key

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.

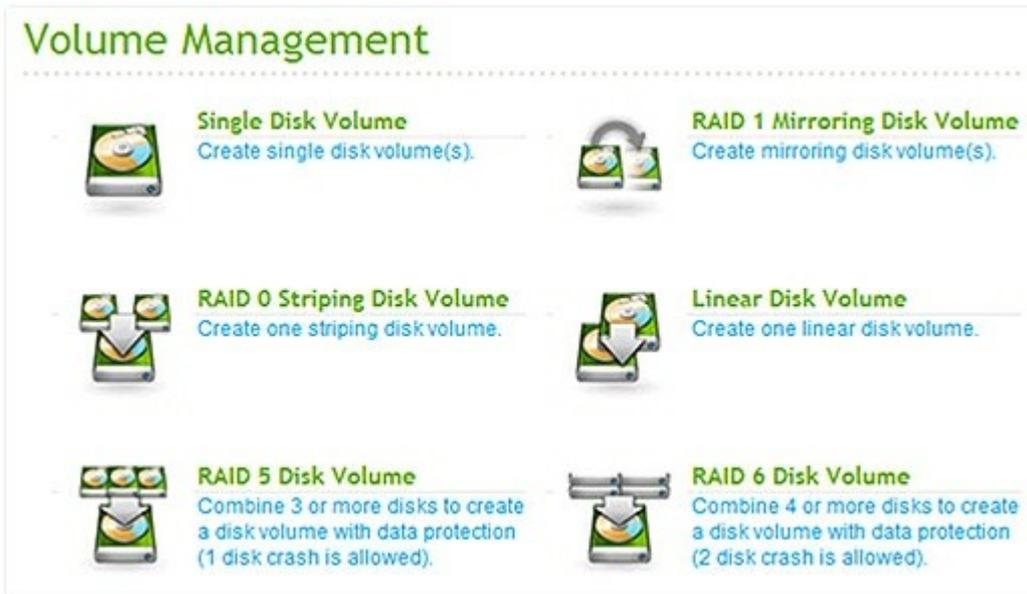
- Use Default Value: Select to use the default encryption password "admin".
- Save Encryption Key: Save the encryption key on the NAS (this option can be changed later).
 - If checked: The NAS will unlock the encrypted disk volume automatically using the saved password when it starts up.
 - If not checked: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

Disk	Model	Capacity	Status	
<input type="checkbox"/>	Drive 2	SAMSUNG HD502HI 1AG0	465.76 GB	Ready
<input checked="" type="checkbox"/>	Drive 5	Seagate ST3500320NS SN16	465.76 GB	Ready

Encryption: **No** ▼

File System: **EXT4** ▼

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

Disk	Model	Capacity	Status	
<input type="checkbox"/>	Drive 2	SAMSUNG HD502HI 1AG0	465.76 GB	Ready
<input checked="" type="checkbox"/>	Drive 5	Seagate ST3500320NS SN16	465.76 GB	Ready

Encryption **Yes** ▼

Input Encryption Password: ●●●●●●●●

Verify Encryption Password: ●●●●●●●●

Use Default Value Save Encryption Key

File System: **EXT4** ▼

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.

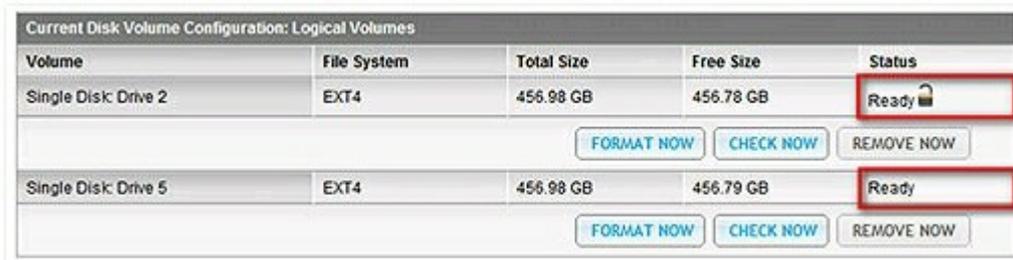


You have created a encrypted disk volume on the NAS.

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.



Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 2	EXT4	456.98 GB	456.78 GB	Ready 
				FORMAT NOW CHECK NOW REMOVE NOW
Single Disk: Drive 5	EXT4	456.98 GB	456.79 GB	Ready
				FORMAT NOW CHECK NOW REMOVE NOW

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.

Current Disk Volume Configuration: Logical Volumes				
Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 2	EXT4	456.98 GB	456.78 GB	Ready
FORMAT NOW CHECK NOW REMOVE NOW				
Single Disk: Drive 5	Unknown	--	--	Unmounted
FORMAT NOW CHECK NOW REMOVE NOW				

- 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

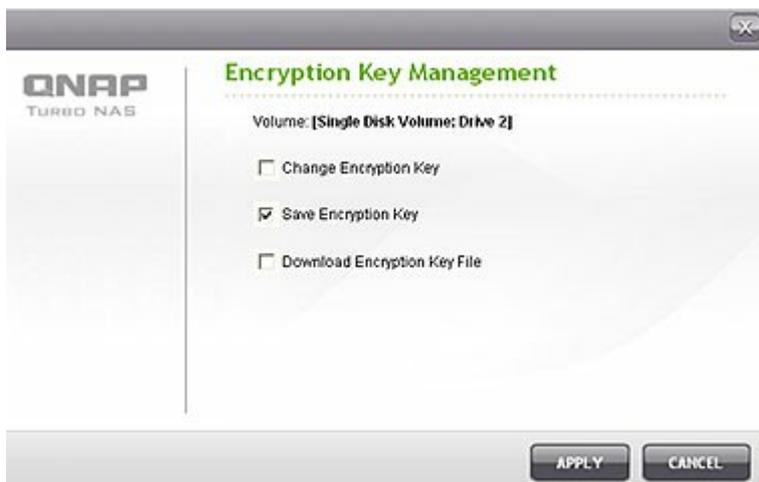
To manage the encryption key settings, login the NAS as an administrator and go to "Disk Management" > "Encrypted File System".

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.

Encryption Key Management

Volume	Total Size	Status	Action
Single Disk: Drive 2	456.98 GB	Unlocked	ENCRYPTION KEY MANAGEMENT
Single Disk: Drive 5	--	Locked	Input Encryption Password <input type="text"/> <input type="button" value="Open"/>

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

Encryption Key Management

Volume	Total Size	Status	Action
Single Disk: Drive 2	456.98 GB	Unlocked	ENCRYPTION KEY MANAGEMENT
Single Disk: Drive 5	--	Locked	Input Encryption Password <input type="text"/> <input type="button" value="Open"/>

Upload Encryption Key File

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

Volume	Total Size	Status	Action
Single Disk: Drive 2	456.98 GB	Unlocked	ENCRYPTION KEY MANAGEMENT
Single Disk: Drive 5	456.98 GB	Unlocked	ENCRYPTION KEY MANAGEMENT

4.5 iSCSI

Portal Management [132](#)

Target Management [143](#)

Advanced ACL [169](#)

LUN Backup [173](#)

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

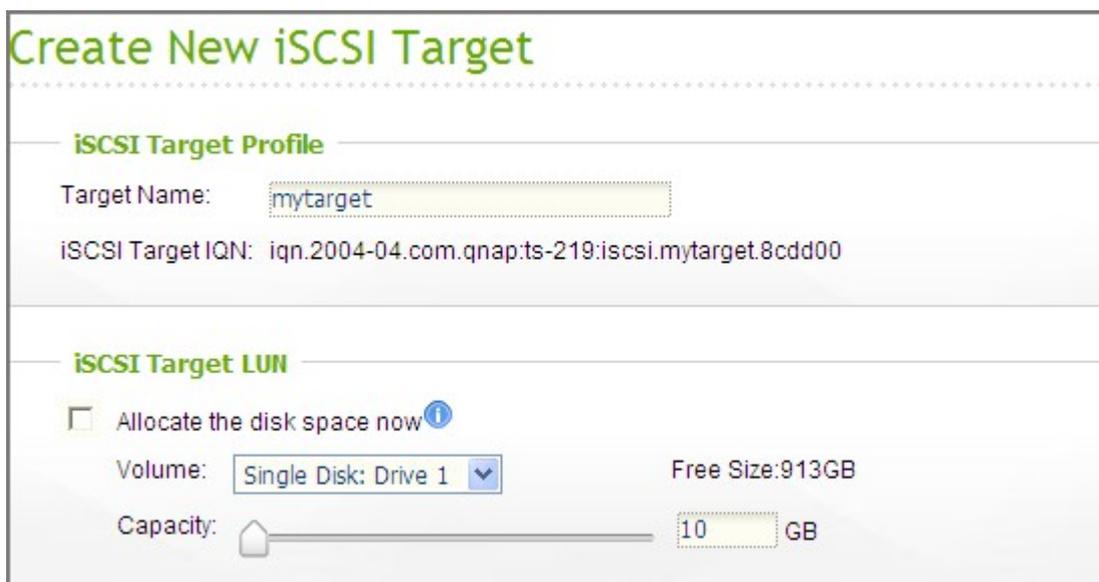
Follow the steps below to create iSCSI targets and LUN on the NAS.

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 username and password settings under "CHAP" only, only the iSCSI target authenticates the initiator. In other words, the initiators have to enter the username 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 username and password. The initiator authenticates the target using the "Mutual CHAP" settings.

Field	Username limitation	Password limitation
Use CHAP authentication	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z Maximum length: 256 characters 	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z Maximum length: 12-16 characters
Mutual CHAP	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) Maximum length: 12-16 characters 	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) Maximum length: 12-16 characters

Type

None

CHAP

User Name: (A~Z, a~z, 0~9)

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

Re-enter Password:

Mutual CHAP

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

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

Re-enter Password:

CRC/Checksum (optional)

Data Digest

Header Digest

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

iSCSI Configuration

iSCSI TARGET LIST

iSCSI Target List

[Create New iSCSI Target](#)

iSCSI Target Name	Capacity	Status	Action
iqn.2004-04.com.qnap.ts-219.iscsi.mytarget.8cdd00	10.00 GB	Offline	

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

iSCSI Portal

Enable iSCSI Target Service
iSCSI Service Port:

Enable iSNS
iSNS Server IP:

APPLY

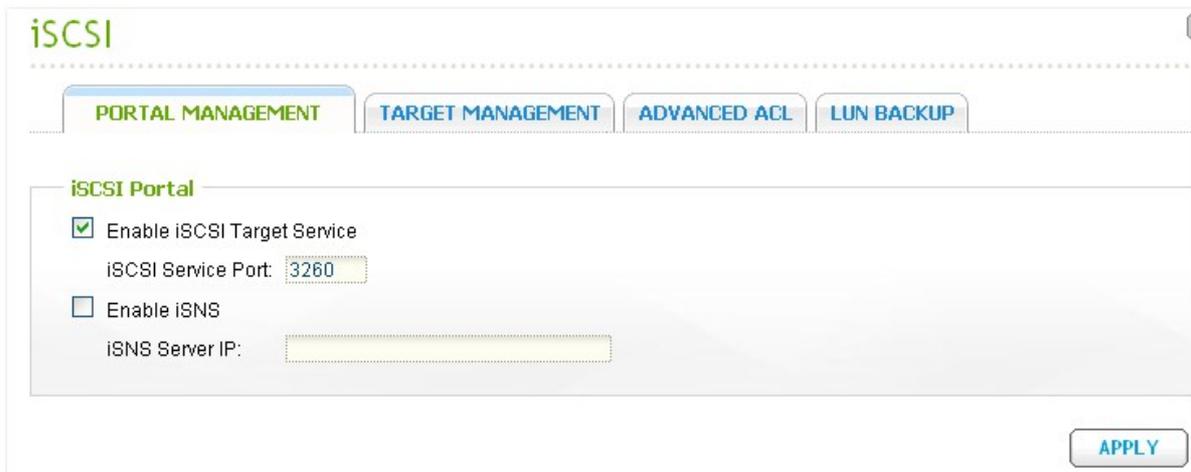
iSCSI Quick Configuration Wizard

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.



The screenshot shows the iSCSI configuration interface. At the top, there are four tabs: "PORTAL MANAGEMENT" (selected), "TARGET MANAGEMENT", "ADVANCED ACL", and "LUN BACKUP". Below the tabs, the "iSCSI Portal" section is visible. It contains the following options:

- Enable iSCSI Target Service
 - iSCSI Service Port:
- Enable iSNS
 - iSNS Server IP:

An "APPLY" button is located at the bottom right of the configuration area.

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.



The image shows a screenshot of the 'iSCSI Quick Configuration Wizard' window. The title bar reads 'iSCSI Quick Configuration Wizard' with a close button on the right. On the left side, there is a logo for 'QNAP TURBO NAS'. The main content area is titled 'Create New iSCSI Target' in green text. Below this title, there is a section for 'iSCSI Target Profile' with three input fields: 'Target Name' containing 'target01', 'iSCSI Target IQN' containing 'iqn.2004-04.com.qnap.ts-809:iscsi.target01.8a000f', and 'Target Alias' containing 'target'. Below these fields is a section for 'CRC/Checksum (optional)' with two unchecked checkboxes: 'Data Digest' and 'Header Digest'. At the bottom of the window, there is a status bar showing 'Step 2 of 6' on the left and three buttons: 'BACK', 'NEXT', and 'CANCEL' on the right.

QNAP
TURBO NAS

Create New iSCSI Target

iSCSI Target Profile

Target Name:

iSCSI Target IQN:

Target Alias:

CRC/Checksum (optional)

Data Digest

Header Digest

Step 2 of 6

BACK NEXT CANCEL

- Enter the CHAP authentication settings. If you enter the username and password settings under "Use CHAP authentication" only, only the iSCSI target authenticates the initiator, i.e. the initiators have to enter the username 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 username and password. The initiator authenticates the target using the "Mutual CHAP" settings.

Field	Username limitation	Password limitation
Use CHAP authentication	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z Maximum length: 256 characters 	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z Maximum length: 12-16 characters
Mutual CHAP	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) Maximum length: 12-16 characters 	<ul style="list-style-type: none"> The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) Maximum length: 12-16 characters

iSCSI Quick Configuration Wizard

QNAP TURBO NAS

CHAP Authentication Settings

Use CHAP authentication

User Name:

Password:

Re-enter Password:

Mutual CHAP

User Name:

Password:

Re-enter Password:

Step 3 of 6

BACK **NEXT** **CANCEL**

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".



The image shows a screenshot of the 'iSCSI Quick Configuration Wizard' window. The title bar reads 'iSCSI Quick Configuration Wizard' with a close button on the right. The main content area is titled 'Create an iSCSI LUN' in green text. On the left side, there is a logo for 'QNAP TURBO NAS'. The configuration options are as follows:

- LUN Allocation:** Two radio buttons are present. 'Thin-Provisioning' is selected (indicated by a filled circle), and 'Instant Allocation' is unselected (indicated by an empty circle). An information icon (i) is next to 'Instant Allocation'.
- LUN Name:** A text input field containing the value '001'.
- LUN Location:** A dropdown menu showing '/share/HDB_DATA' with a downward arrow. To the right of the dropdown, it says 'Free Size: 281.6GB'.
- Capacity:** A slider control with a house-shaped handle. To the right of the slider is a text input field containing '50' followed by 'GB'.

At the bottom of the window, there is a status bar that says 'Step 4 of 6'. On the right side of the status bar, there are three buttons: 'BACK', 'NEXT', and 'CANCEL'.

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.

iSCSI Target List			
	Alias (IQN)	Status	Action
	01 (iqn.2004-04.com:ts-239:iscsi.target01.8cbc6c) └ id:0 - 001 (1.00 GB)	Ready Enabled	    

Total: 1 | Display 10 entries per page.   1 / 1  

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.

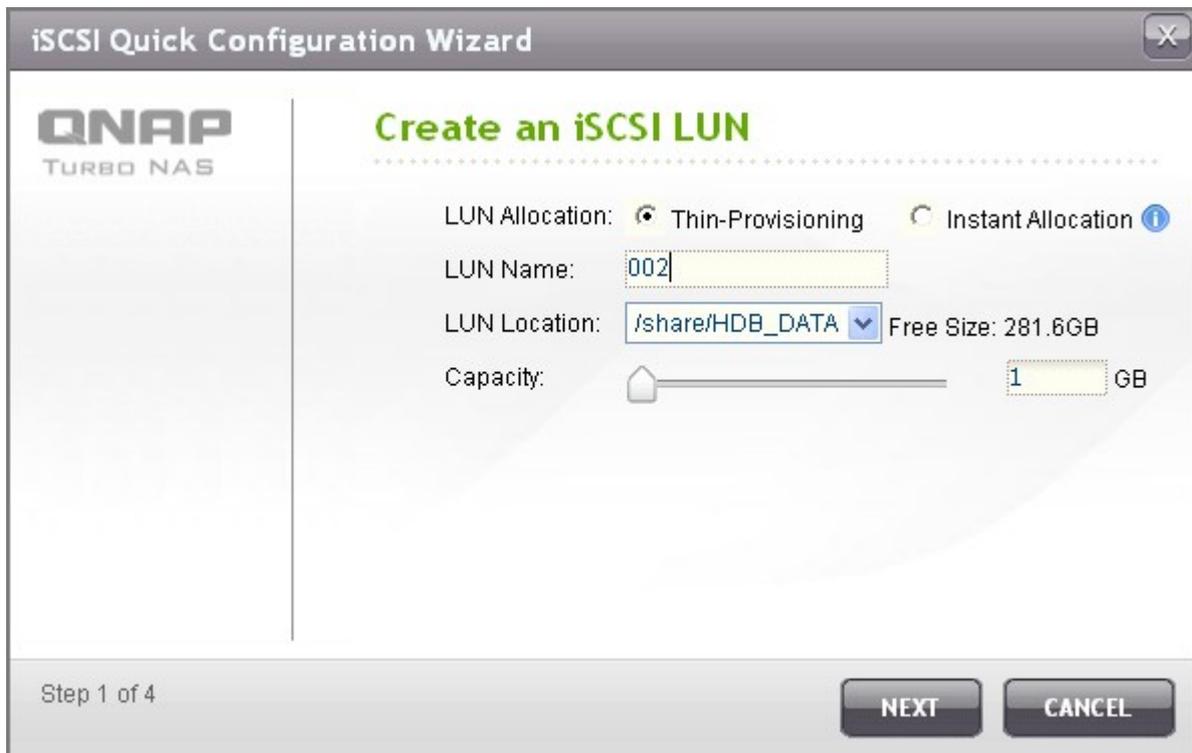
1. Click "Quick Configuration Wizard" under "Target Management".



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".



The image shows a screenshot of the 'iSCSI Quick Configuration Wizard' window. The title bar reads 'iSCSI Quick Configuration Wizard' with a close button (X) on the right. On the left side, there is a logo for 'QNAP TURBO NAS'. The main content area is titled 'Create an iSCSI LUN' in green text. Below the title, there are four configuration fields: 1. 'LUN Allocation:' with two radio buttons: 'Thin-Provisioning' (selected) and 'Instant Allocation' (with an information icon). 2. 'LUN Name:' with a text input field containing '002'. 3. 'LUN Location:' with a dropdown menu showing '/share/HDB_DATA' and a 'Free Size: 281.6GB' label. 4. 'Capacity:' with a slider bar and a text input field containing '1' followed by 'GB'. At the bottom left, it says 'Step 1 of 4'. At the bottom right, there are two buttons: 'NEXT' and 'CANCEL'.

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



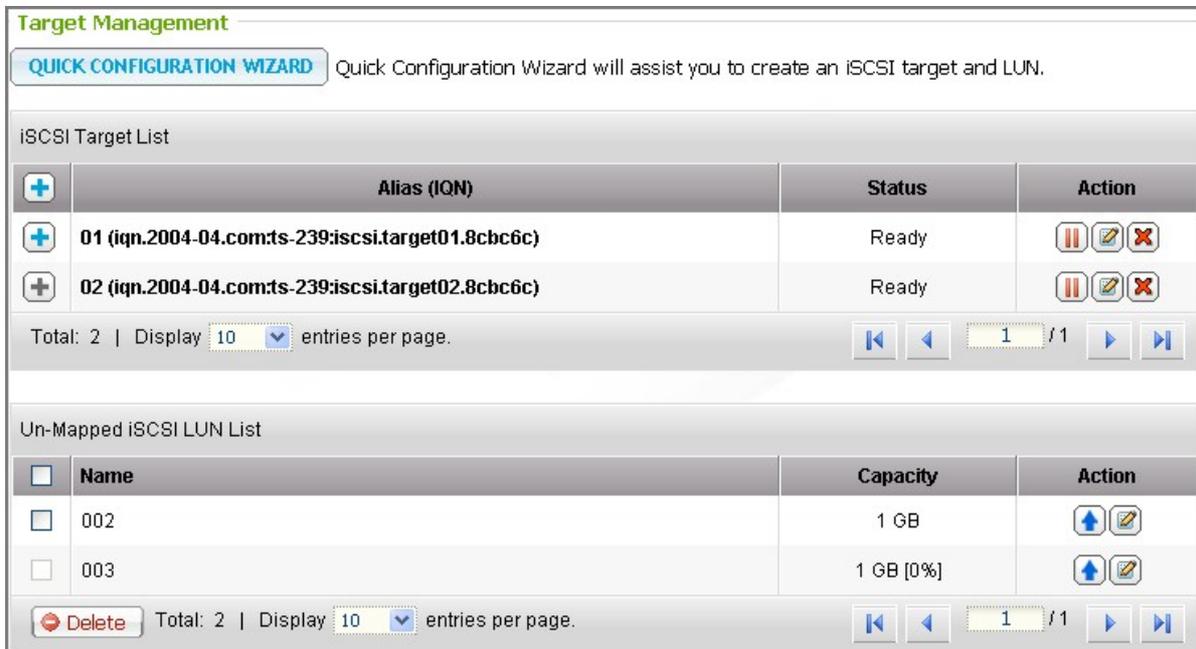
5. Confirm the settings and click "Next".



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.

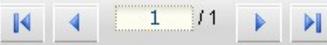
Follow the steps below to switch the mapping of an iSCSI LUN.

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

iSCSI Target List			
	Alias (IQN)	Status	Action
	01 (iqn.2004-04.com:ts-239:iscsi.target01.8cbc6c) └ id:0 - 001 (1.00 GB)	Ready Enabled	    

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.

iSCSI Target List			
	Alias (IQN)	Status	Action
	01 (iqn.2004-04.com:ts-239:iscsi.target01.8cbc6c) └ id:0 - 001 (1.00 GB)	Ready Disabled	     
	02 (iqn.2004-04.com:ts-239:iscsi.target02.8cbc6c)	Ready	  
Total: 2 Display 10 entries per page. 			
Un-Mapped iSCSI LUN List			
<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	002	1 GB	 

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



4. The LUN is mapped to the target.

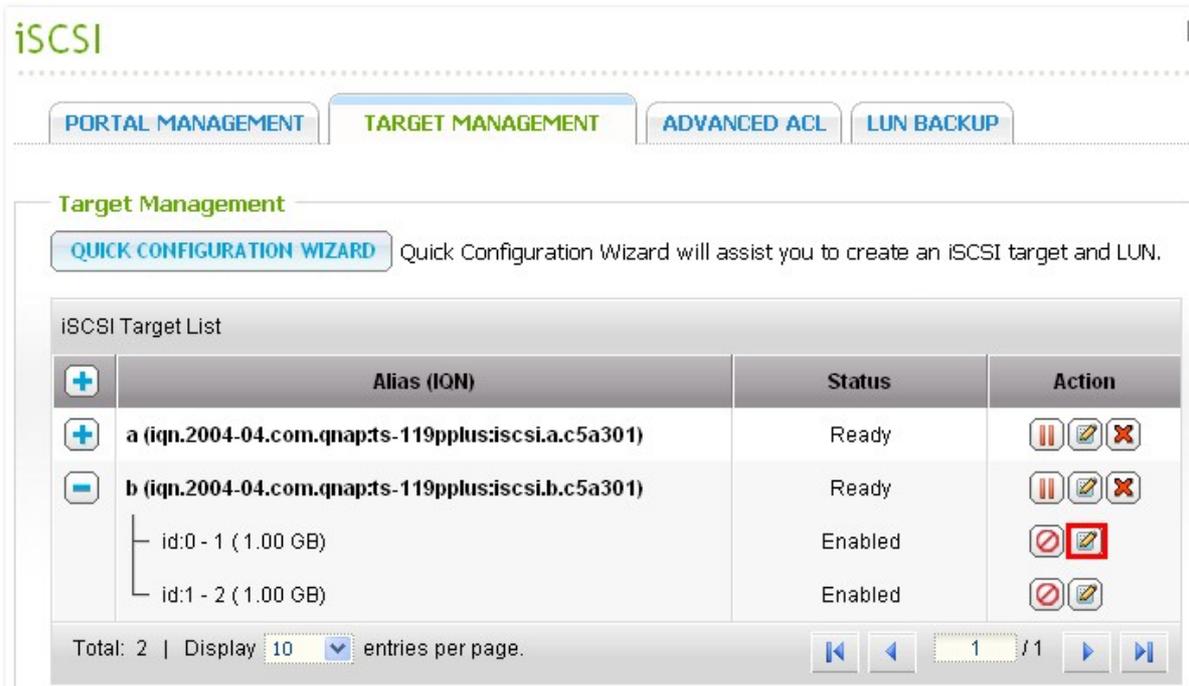
iSCSI Target List			
	Alias (IQN)	Status	Action
<input checked="" type="checkbox"/>	01 (iqn.2004-04.com:ts-239:iscsi.target01.8cbc6c)	Ready	  
	└ id:0 - 002 (1.00 GB)	Enabled	 

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 .



The screenshot shows the iSCSI management interface. At the top, there are tabs for PORTAL MANAGEMENT, TARGET MANAGEMENT (selected), ADVANCED ACL, and LUN BACKUP. Below the tabs, there is a 'Target Management' section with a 'QUICK CONFIGURATION WIZARD' button and a description: 'Quick Configuration Wizard will assist you to create an iSCSI target and LUN.' Below this is the 'iSCSI Target List' table.

	Alias (IQN)	Status	Action
	a (iqn.2004-04.com.qnap:ts-119pplus:iscsi.a.c5a301)	Ready	  
	b (iqn.2004-04.com.qnap:ts-119pplus:iscsi.b.c5a301)	Ready	  
	id:0 - 1 (1.00 GB)	Enabled	 
	id:1 - 2 (1.00 GB)	Enabled	 

Total: 2 | Display 10 entries per page. 

- 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

Modify an iSCSI LUN

LUN Allocation: Thin Provisioning i
 Instant Allocation

LUN Name:

LUN Location:
Free Size: 408.19 GB

LUN Serial Number: 7184c7aa-2f42-4d0e-aa3e-9625f0e977a2

Capacity: 32768 GB

APPLY **CANCEL**

- Click "Apply" to save the settings.

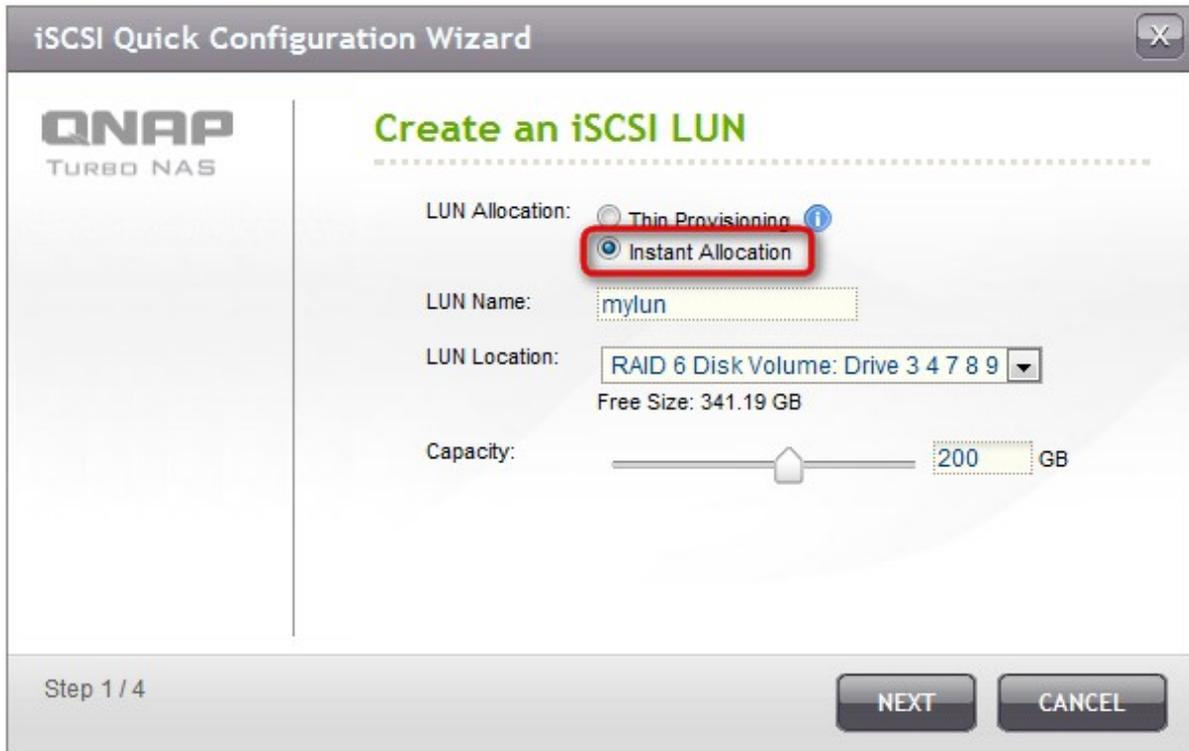
Note: An iSCSI LUN must be mapped to an iSCSI target before increasing the capacity.

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:

1. 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.



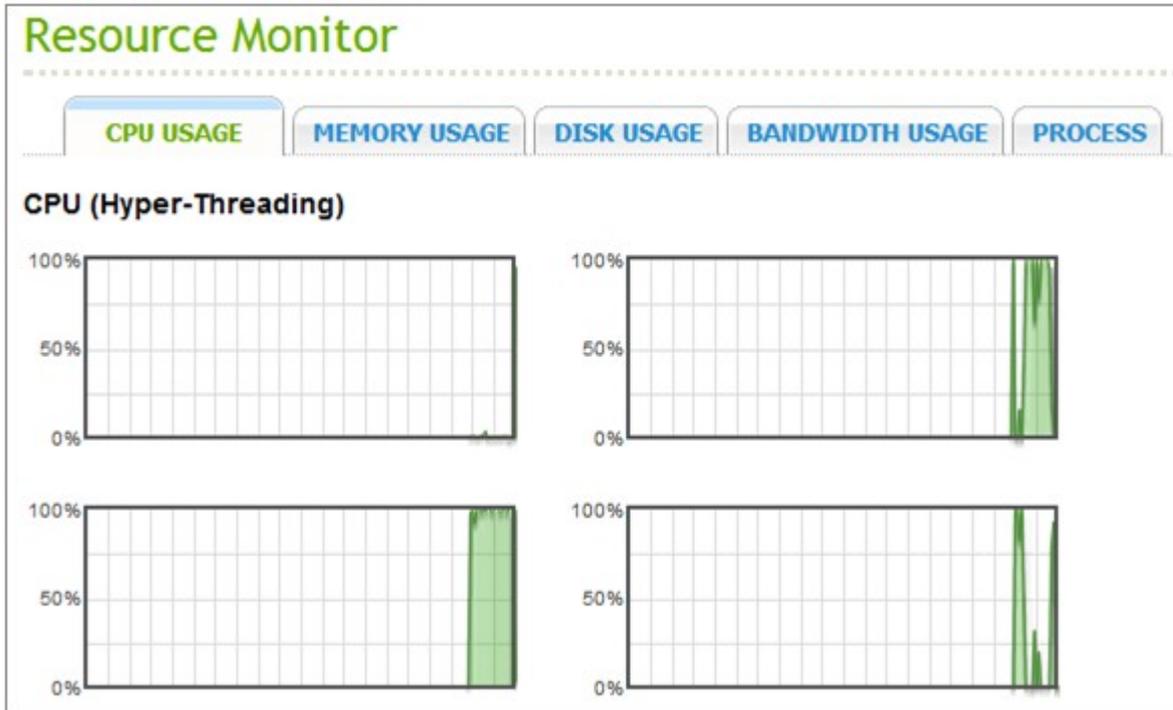
The screenshot shows the 'iSCSI Quick Configuration Wizard' window. The title bar reads 'iSCSI Quick Configuration Wizard' with a close button (X) on the right. The main content area is titled 'Create an iSCSI LUN' in green. On the left side, there is a logo for 'QNAP TURBO NAS'. The configuration options are as follows:

- LUN Allocation:** Two radio buttons are present: 'Thin Provisioning' (unselected) and 'Instant Allocation' (selected). The 'Instant Allocation' option is highlighted with a red rectangular box.
- LUN Name:** A text input field containing 'mylun'.
- LUN Location:** A dropdown menu showing 'RAID 6 Disk Volume: Drive 3 4 7 8 9'.
- Free Size:** A label indicating '341.19 GB'.
- Capacity:** A slider control with a numerical input field set to '200' and the unit 'GB'.

At the bottom of the wizard, it indicates 'Step 1 / 4' on the left and two buttons, 'NEXT' and 'CANCEL', on the right.

2. 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.



3. 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

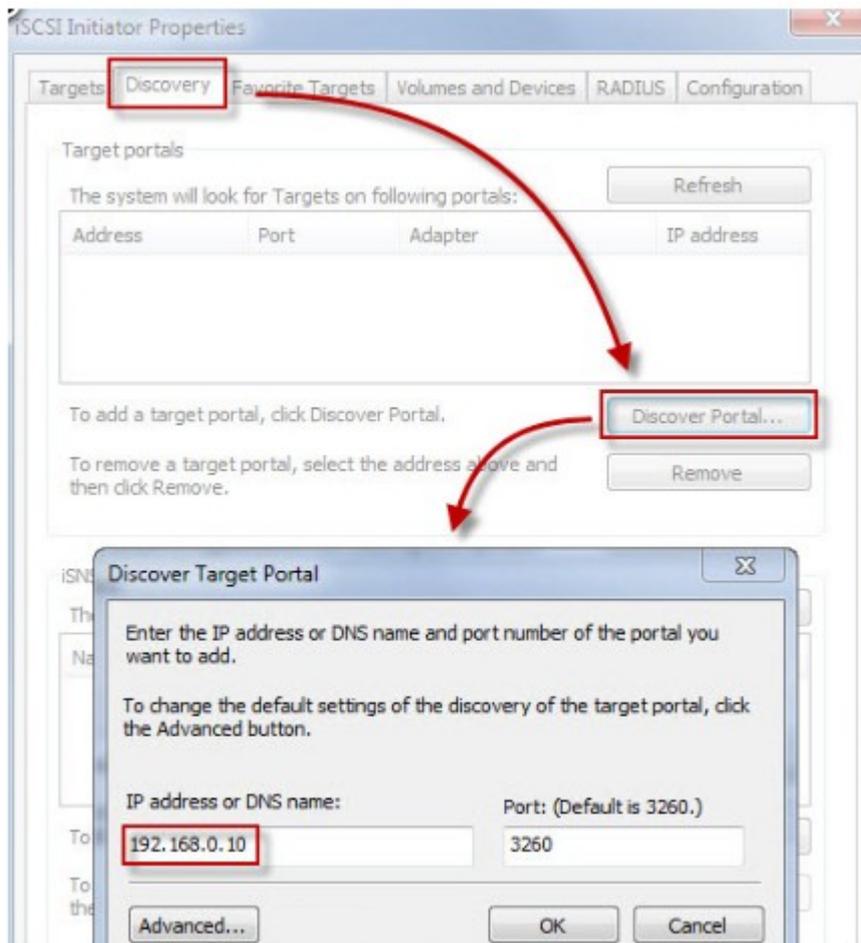
Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

iSCSI initiator on Windows

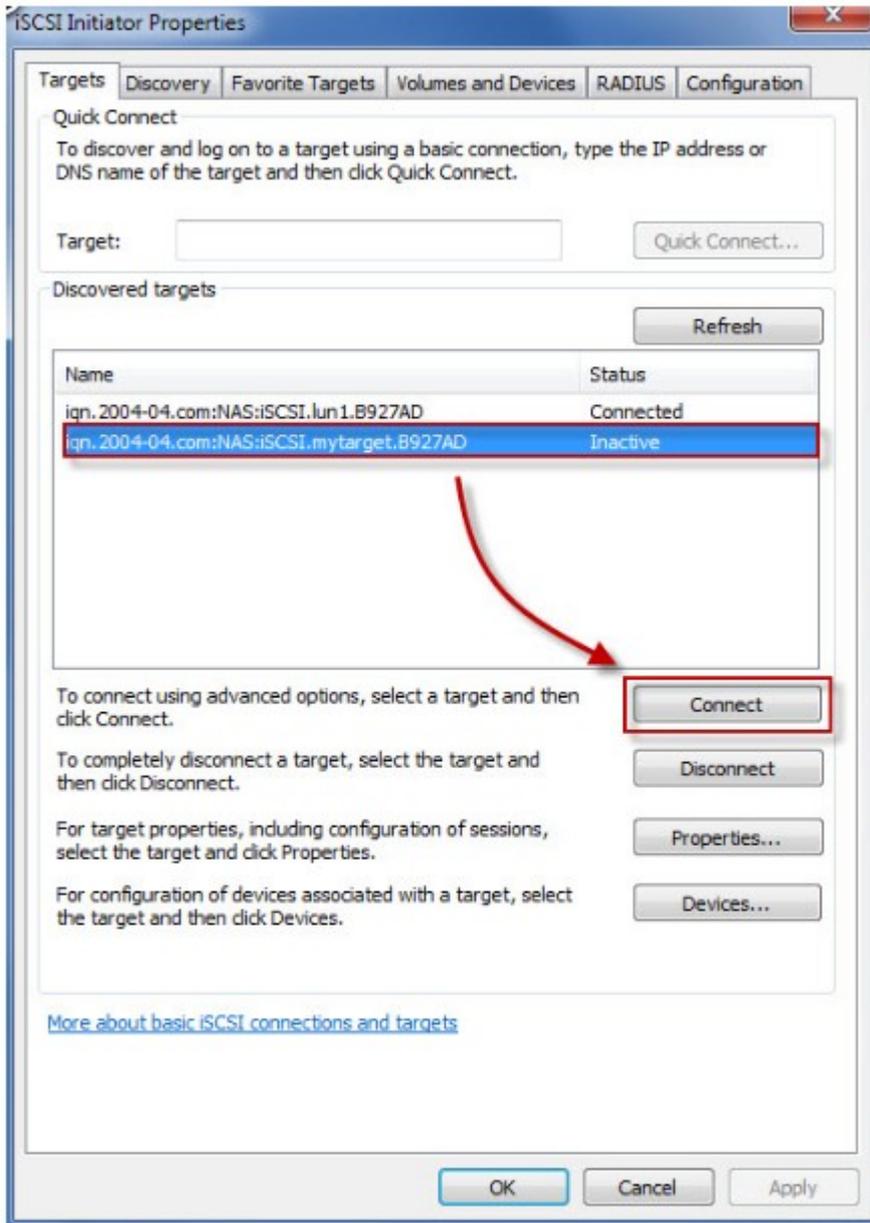
Microsoft iSCSI Software Initiator v2.07 is an official application for Windows OS 2003, XP, and 2000 to allow users to implement an external iSCSI storage array over the network. If you are using Windows Vista or Windows Server 2008, Microsoft iSCSI Software Initiator is included. For more information and the download location, visit:

<http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en>

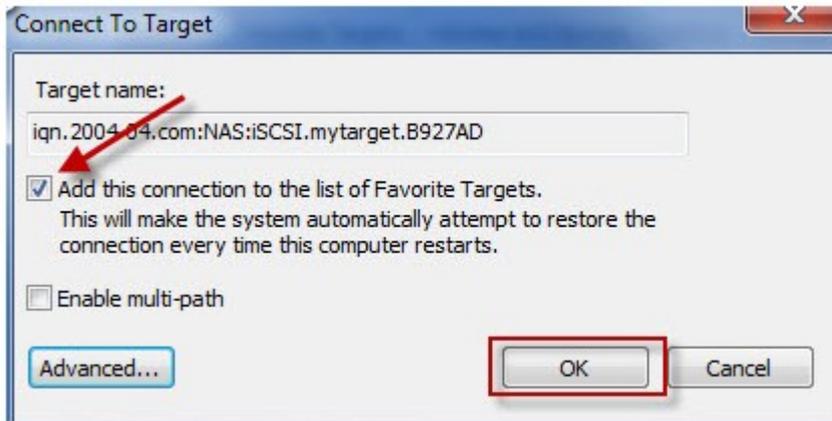
Start iSCSI initiator from "Control Panel" > "Administrative Tools". Under the "Discovery" tab click "Add Portal". Enter the NAS IP and the port number for the iSCSI service.



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".



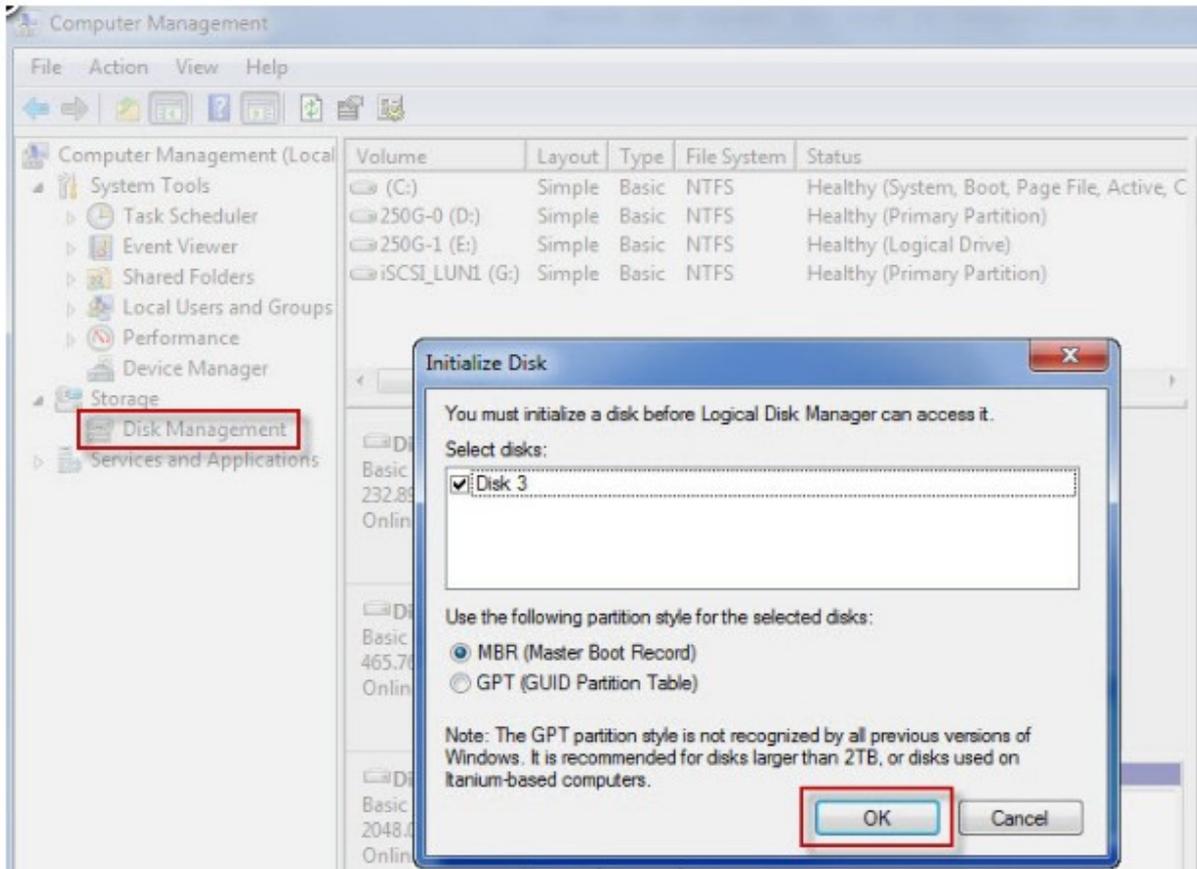
You may click "Advanced" to specify the logon information if you have configured the authentication otherwise simply click "OK" to continue.



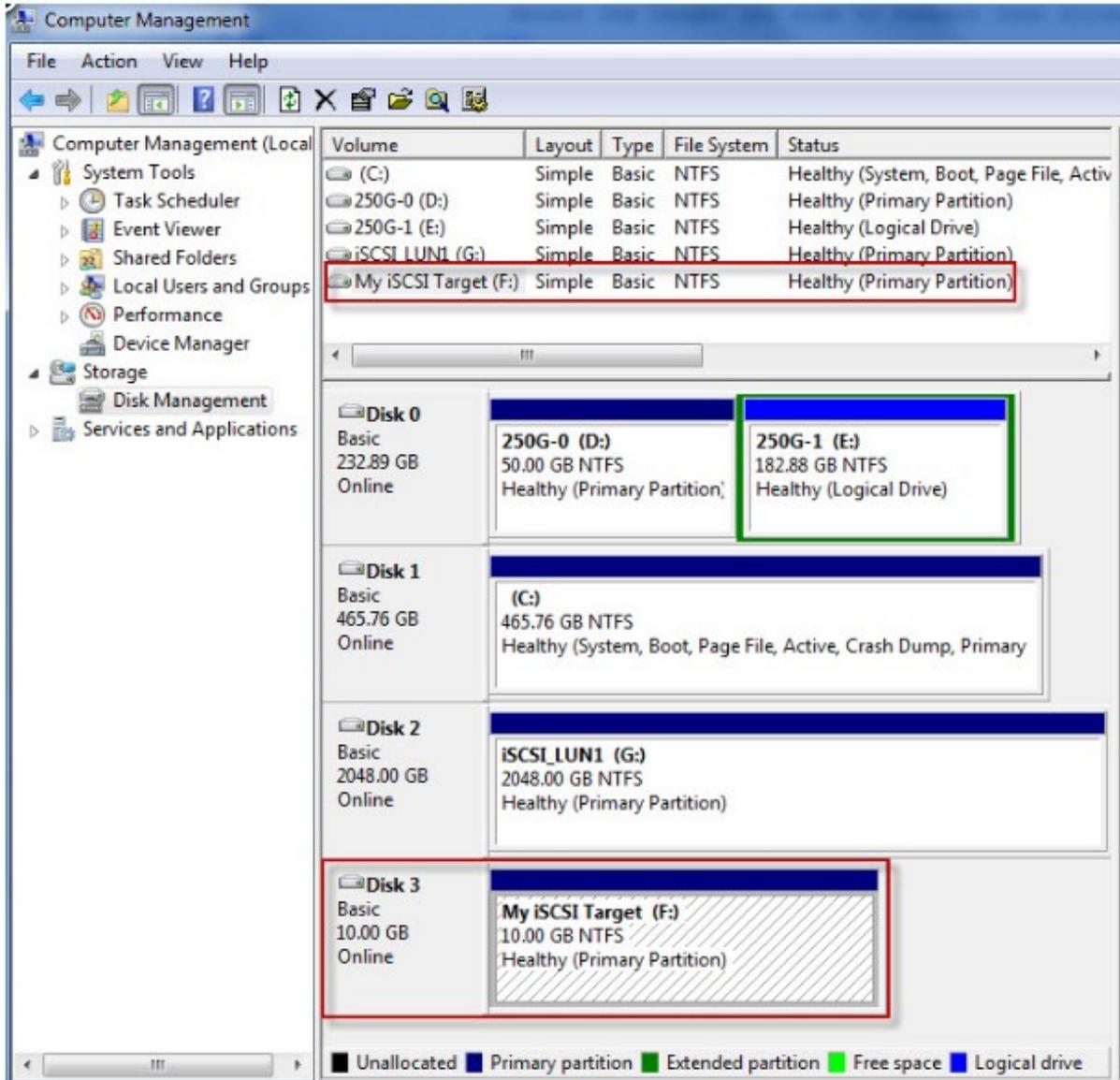
Upon successful logon, the status of the target now shows "Connected".

Name	Status
iqn.2004-04.com:NAS:iSCSI.lun1.B927AD	Connected
iqn.2004-04.com:NAS:iSCSI.mytarget.B927AD	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

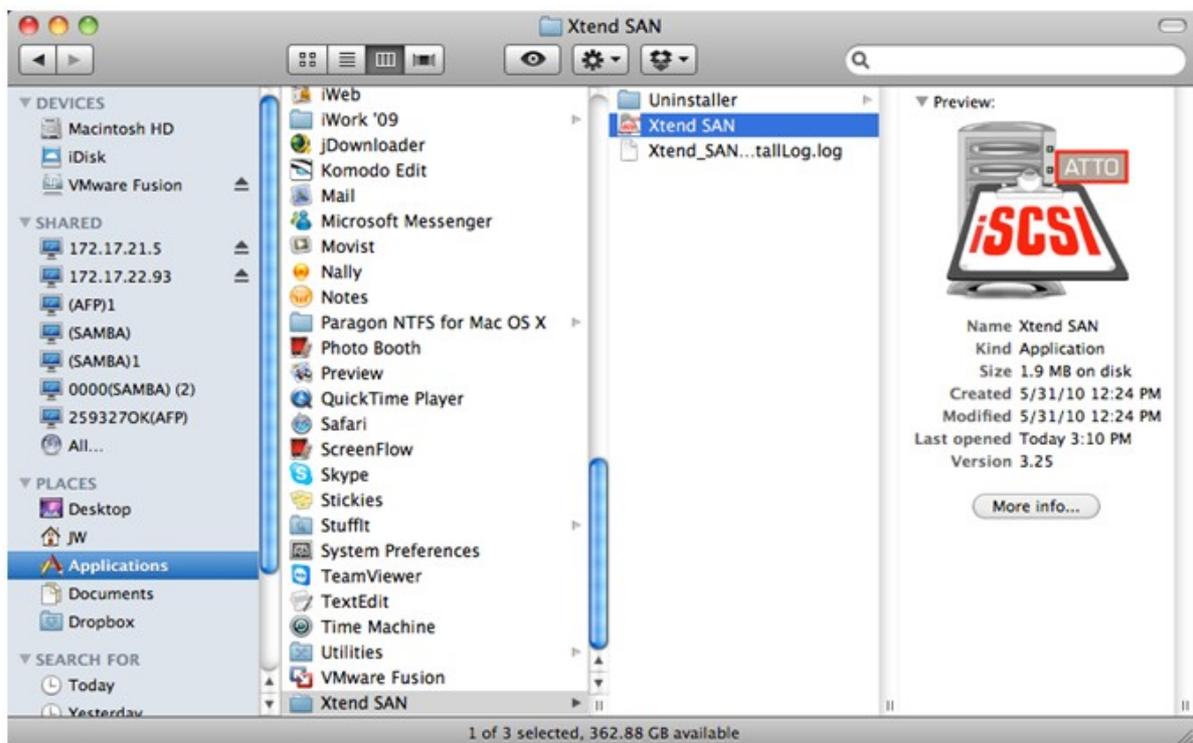
This section shows you how to use Xtend SAN iSCSI Initiator on Mac OS to add the iSCSI target (QNAP NAS) as an extra partition. Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

About Xtend SAN iSCSI initiator

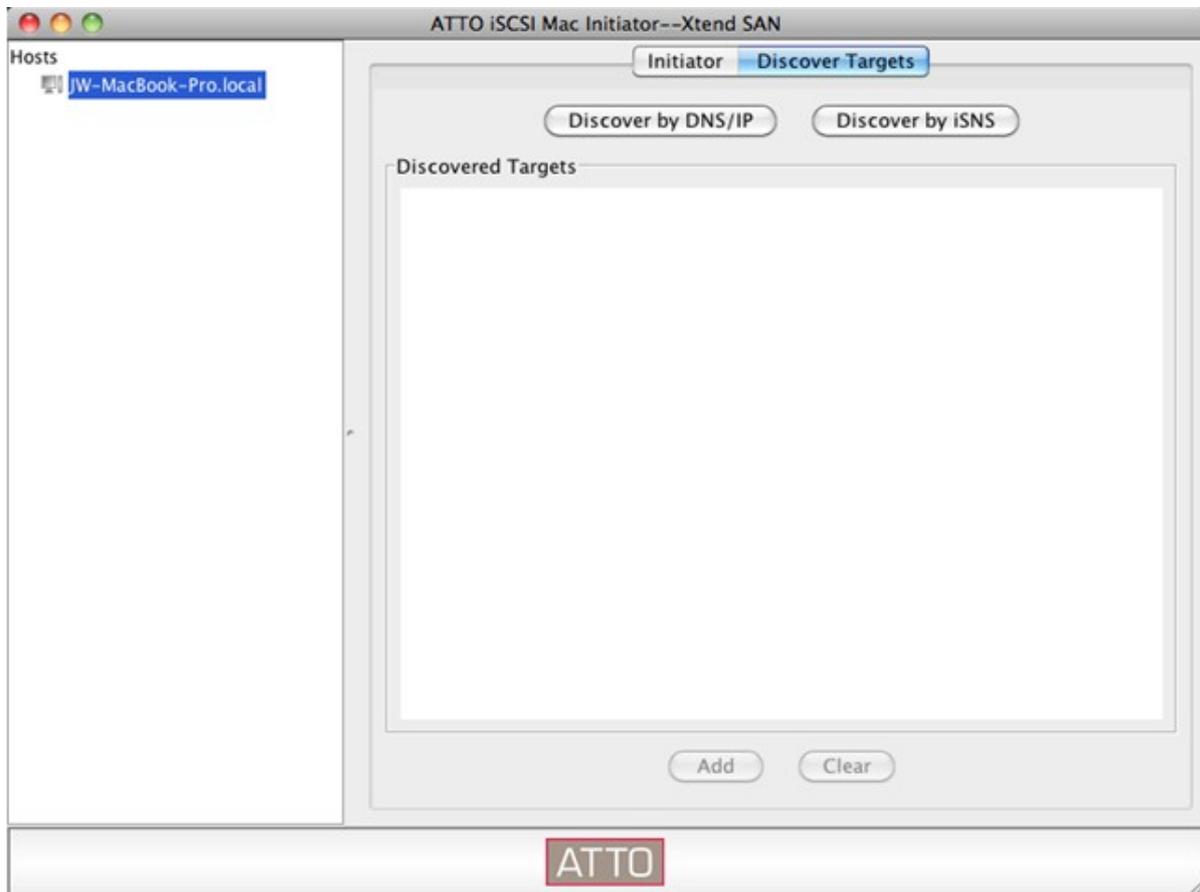
ATTO's Xtend SAN iSCSI Initiator for Mac OS X allows Mac users to utilize and benefit from iSCSI. It is compatible with Mac OS X 10.4.x to 10.6.x. For more information, please visit:

<http://www.attotech.com/products/product.php?sku=INIT-MAC0-001>

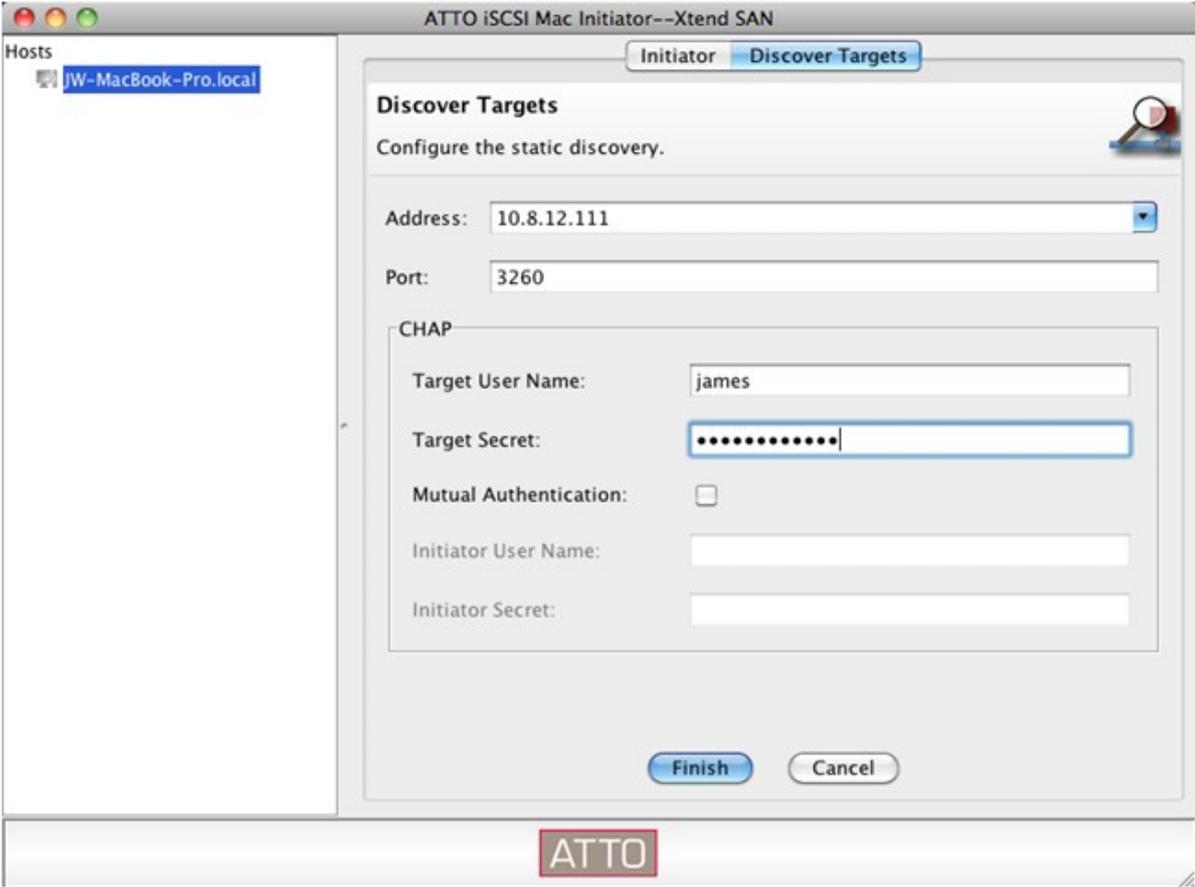
After installing Xtend SAN iSCSI initiator, you can find it in "Applications".



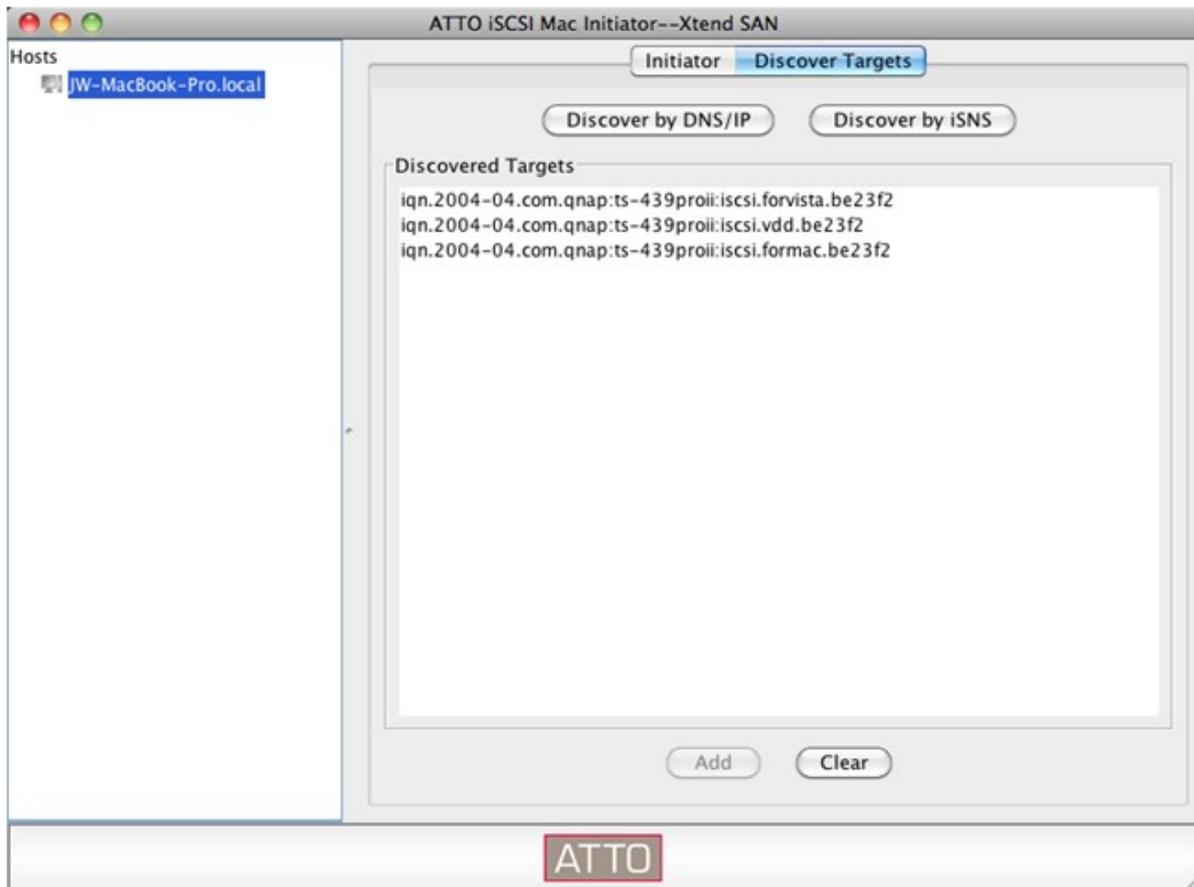
Click the "Discover Targets" tab, you can either choose "Discover by DNS/IP" or "Discover by iSNS" according to the network topology. In this example, we will use the IP address to discover the iSCSI targets.



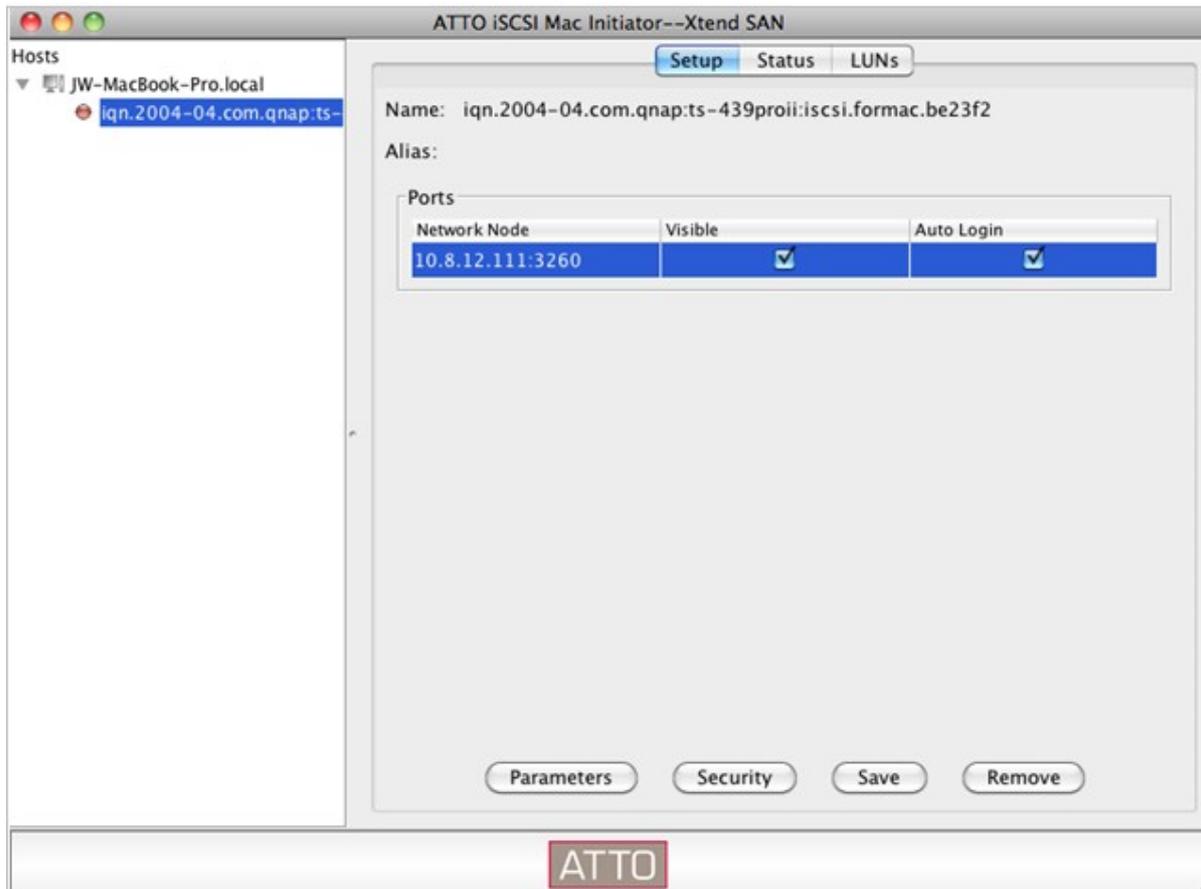
Follow the screen instructions and enter the server address, iSCSI target port number (default: 3260), and CHAP information (if applicable). Click "Finish" to retrieve the target list after all the data have been entered correctly.



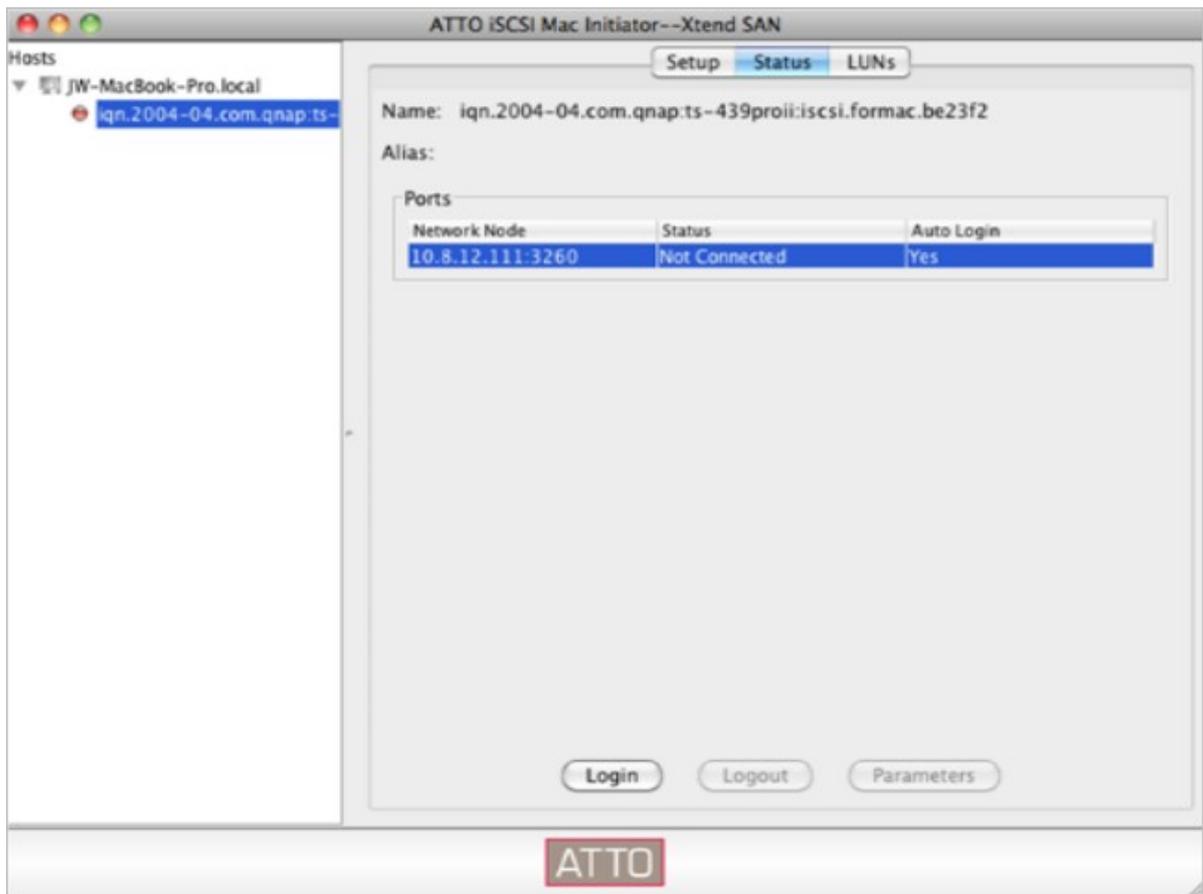
All the available iSCSI targets on the NAS will be shown. Select the target you would like to connect and click "Add".



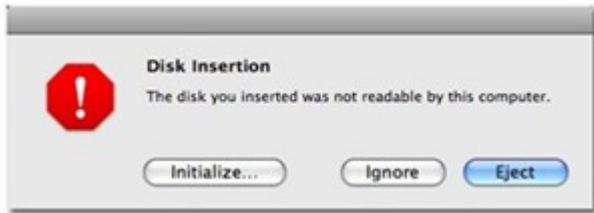
You can configure the connection properties of the selected iSCSI target in the "Setup" tab.



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".

The screenshot shows the 'iSCSI' management interface with the 'ADVANCED ACL' tab selected. Under the 'LUN Masking' section, there is a descriptive paragraph and a table for the 'LUN Masking Policy List'. The table contains one entry, 'Default Policy', with a checkbox, an edit icon, and a delete icon. Below the table is a pagination control showing 'Total: 1 | Display 10 entries per page.' and navigation buttons.

iSCSI

PORTAL MANAGEMENT TARGET MANAGEMENT **ADVANCED ACL** LUN BACKUP

LUN Masking

A connected iSCSI initiator is authenticated by Target ACL and LUN Masking in order to access the iSCSI LUNs mapped to the iSCSI targets on the NAS. (For detailed instructions, please click [here](#))

LUN Masking Policy List Add a Policy

<input type="checkbox"/>	Policy Name	IQN	Action
<input type="checkbox"/>	Default Policy		

Delete Total: 1 | Display 10 entries per page. 1 / 1

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.

Add a Policy ✕

Define the LUN Masking policy for the initiator you input below.

Policy Name:

Initiator IQN:

Name	Read Only	Read/Write	Deny Access
000	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
001	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
002	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
abb	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

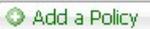
APPLY

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.

LUN Masking

A connected iSCSI initiator is authenticated by Target ACL and LUN Masking in order to access the iSCSI LUNs mapped to the iSCSI targets on the NAS. (For detailed instructions, please click [here](#))

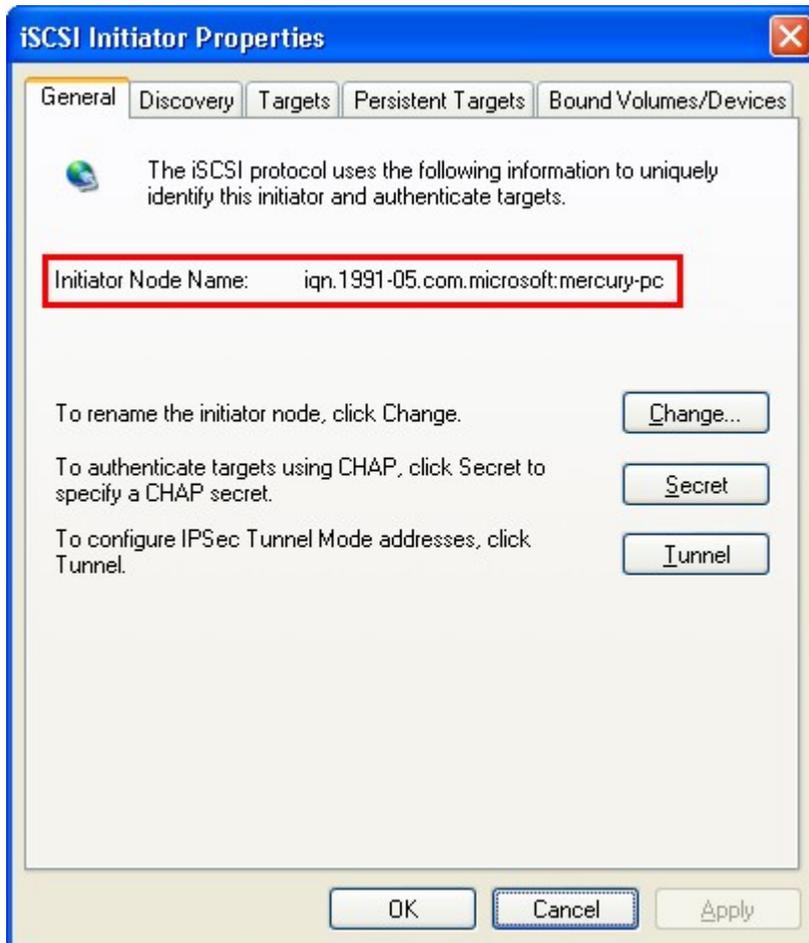
LUN Masking Policy List 

<input type="checkbox"/>	Policy Name	IQN	Action
<input type="checkbox"/>	Default Policy		

 Total: 1 | Display entries per page. 

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.



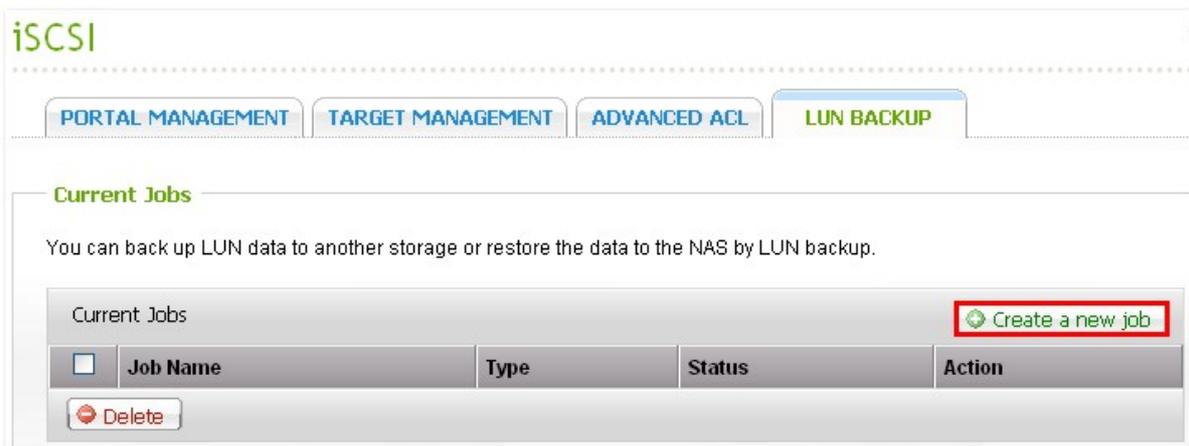
4.5.4 LUN Backup

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".



The screenshot shows the iSCSI management interface. At the top, there are four tabs: PORTAL MANAGEMENT, TARGET MANAGEMENT, ADVANCED ACL, and LUN BACKUP. The LUN BACKUP tab is selected. Below the tabs, there is a section titled "Current Jobs" with a sub-header "Current Jobs". Below this, there is a text box that says "You can back up LUN data to another storage or restore the data to the NAS by LUN backup." Below the text box, there is a table with the following columns: Job Name, Type, Status, and Action. The table is currently empty. To the right of the table, there is a button labeled "Create a new job" with a green plus icon, which is highlighted with a red box. Below the table, there is a "Delete" button with a red minus icon.

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.



- 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".

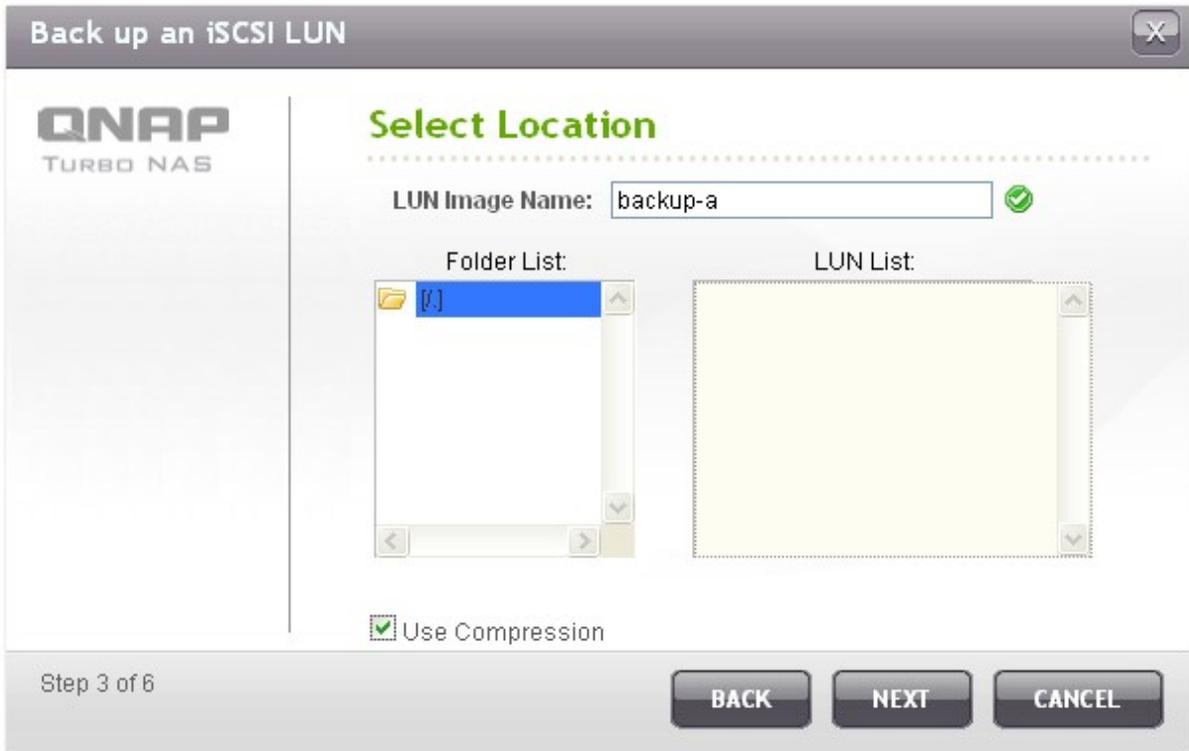
The screenshot shows a window titled "Back up an iSCSI LUN" with a close button in the top right corner. On the left side, there is the QNAP TURBO NAS logo. The main area is titled "Select Destination" in green text. Below the title, there are four fields:

- Protocol:** A dropdown menu showing "Linux Share (NFS)".
- IP Address/Host Name:** A text input field containing a redacted IP address, followed by a green checkmark icon. Below it, examples are listed: "(Examples: 192.168.0.100, nas.com, nas,...)".
- Folder or Path:** A text input field containing "/Public/Backup", followed by a green checkmark icon. Below it, examples are listed: "(Examples: /share/HDA_data/backup)".
- Remote Host Testing:** A button labeled "TEST".

At the bottom left, it says "Step 2 of 6". At the bottom right, there are three buttons: "BACK", "NEXT", and "CANCEL".

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".

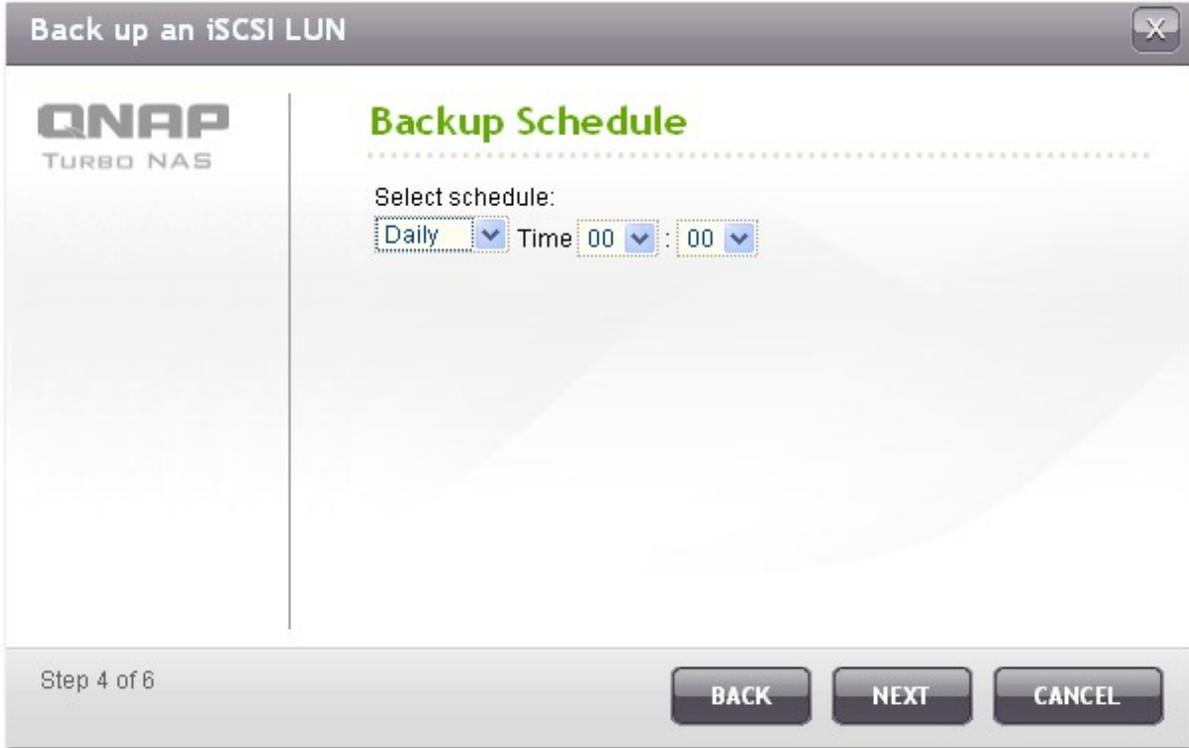
*Use Compression: When this option is enabled, more CPU resources of the NAS will be consumed but the size of the backup LUN can be reduced. The backup time may vary depending on the size of the iSCSI LUN.



6. Specify the backup schedule. The options available are:

- Now
- Hourly
- Daily
- Weekly
- Monthly

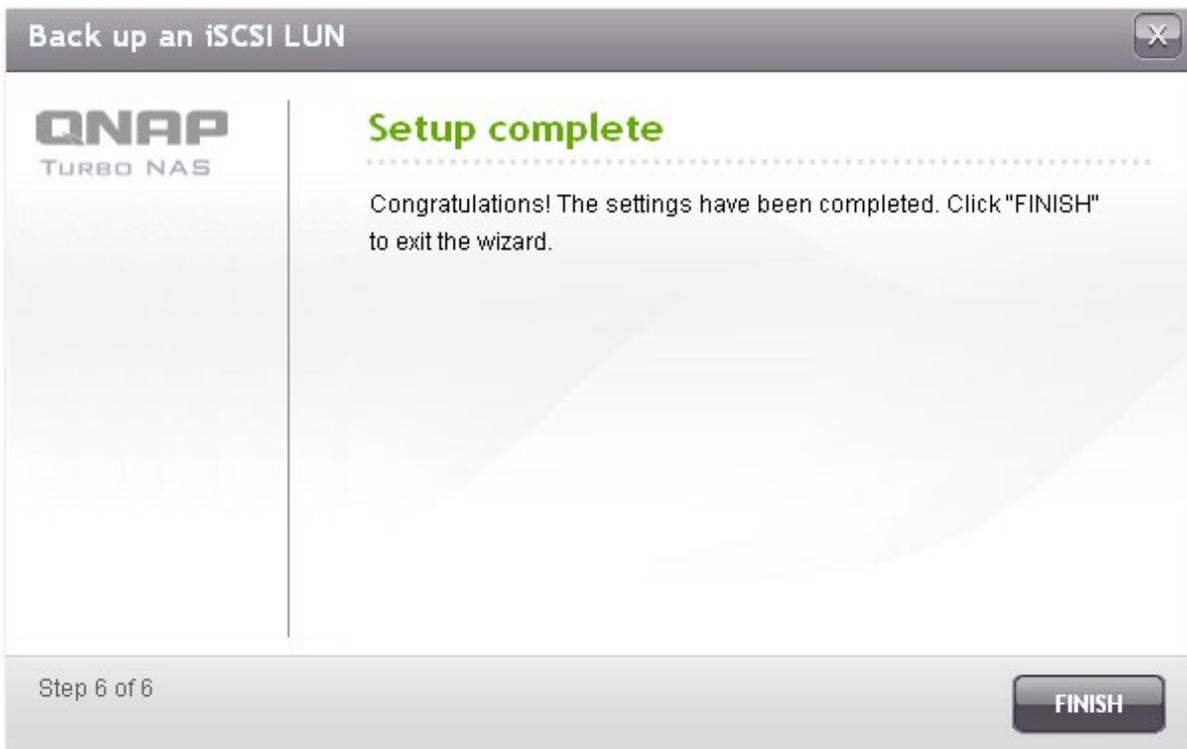
Click "Next".



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.

Current Jobs

You can back up LUN data to another storage or restore the data to the NAS by LUN backup.

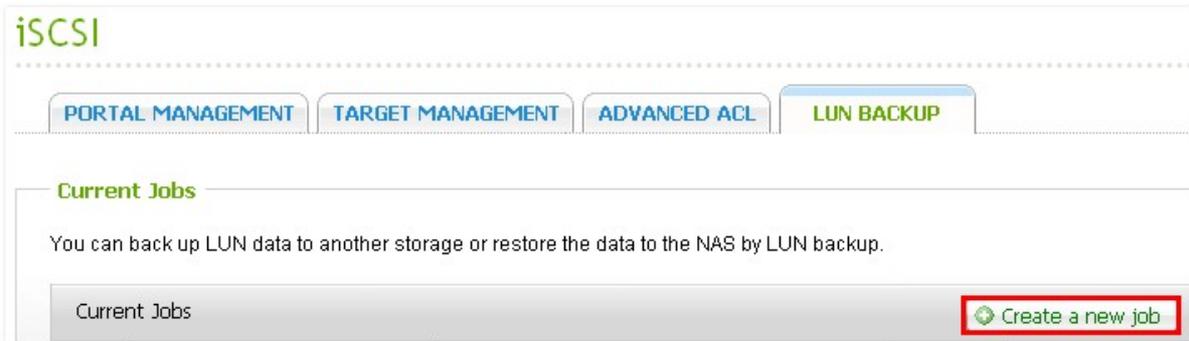
Current Jobs [Create a new job](#)

<input type="checkbox"/>	Job Name	Type	Status	Action
<input type="checkbox"/>	Backup_a->backup-a	Back up (Schedule: Daily 00 : 00)	---	  

[Delete](#)

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".



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

Restore an iSCSI LUN

QNAP
TURBO NAS

Select the restore source

Protocol: Linux Share (NFS) ✓

IP Address/Host Name: [REDACTED] ✓
(Examples: 192.168.0.100, nas.com, nas,...)

Folder or Path: /Public/Backup ✓
(Examples: /share/HDA_data/backup)

Remote Host Testing: **TEST**

Step 1 of 5

NEXT **CANCEL**

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

Restore an iSCSI LUN

QNAP
TURBO NAS

Select Source Location

Folder List: [/]

LUN List: backup-a (a:1.00GB)

Step 2 of 5

BACK **NEXT** **CANCEL**

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".

Restore an iSCSI LUN

QNAP
TURBO NAS

Select Destination

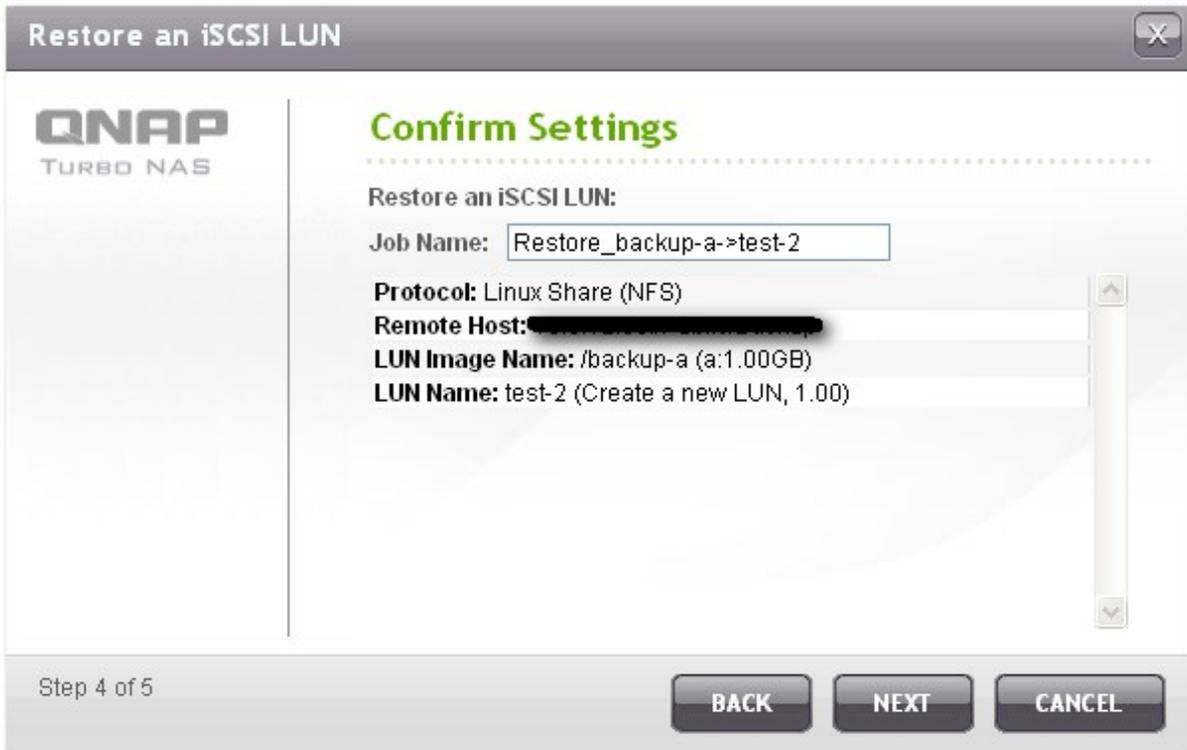
Overwrite existing LUN
a (1.00 GB, Enabled) Free Size: 276.21 GB
Warning: The LUN is busy.
Note: The original data on the LUN will be overwritten.

Create a new LUN
LUN Name: test-2 ✓
LUN Location: Single Disk: Drive 1
Free Size: 275.65 GB

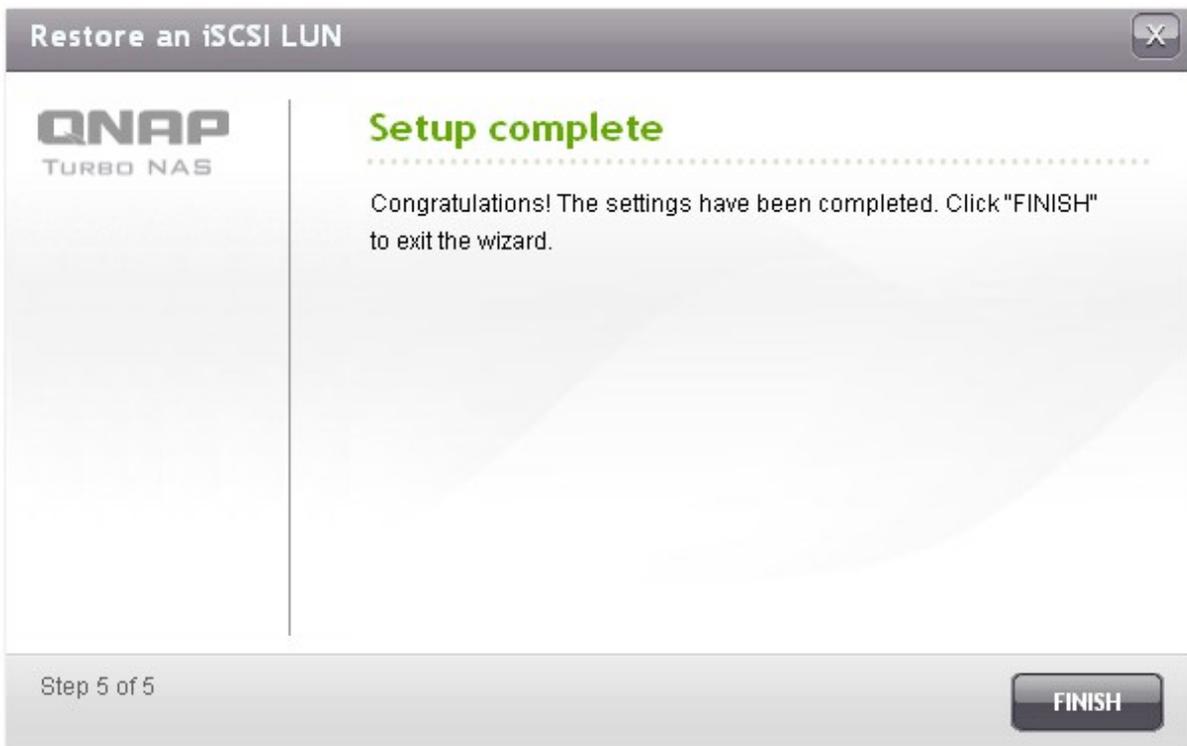
Step 3 of 5

BACK NEXT CANCEL

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



- 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.

Current Jobs

You can back up LUN data to another storage or restore the data to the NAS by LUN backup.

Current Jobs [Create a new job](#)

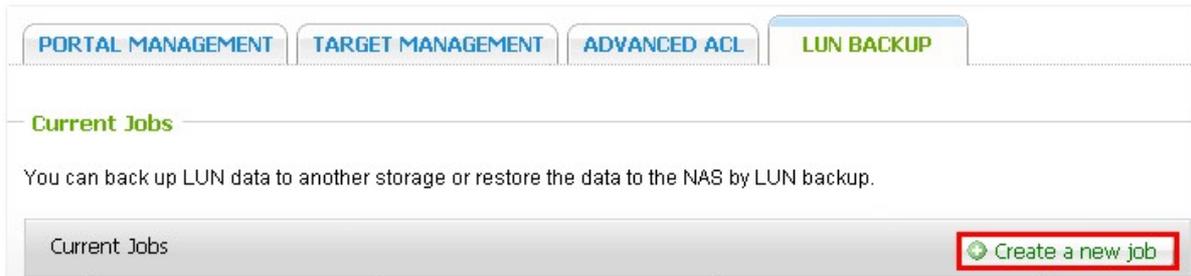
<input type="checkbox"/>	Job Name	Type	Status	Action
<input type="checkbox"/>	Backup_a->backup-a	Back up (Schedule: Daily 00 : 00)	Finished (2011/08/10 15:01:06)	  
<input type="checkbox"/>	Restore_backup-a->test-2	Recovery	Processing... 0 %	  

[Delete](#)

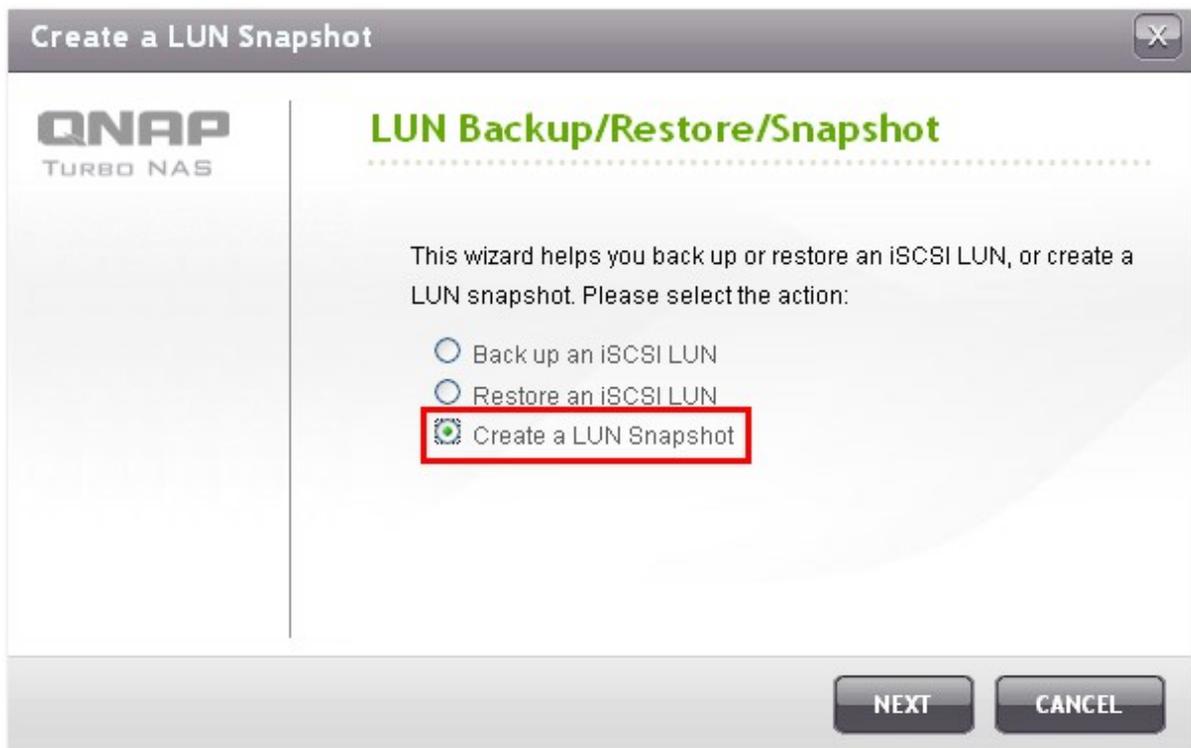
Create an iSCSI LUN Snapshot

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".

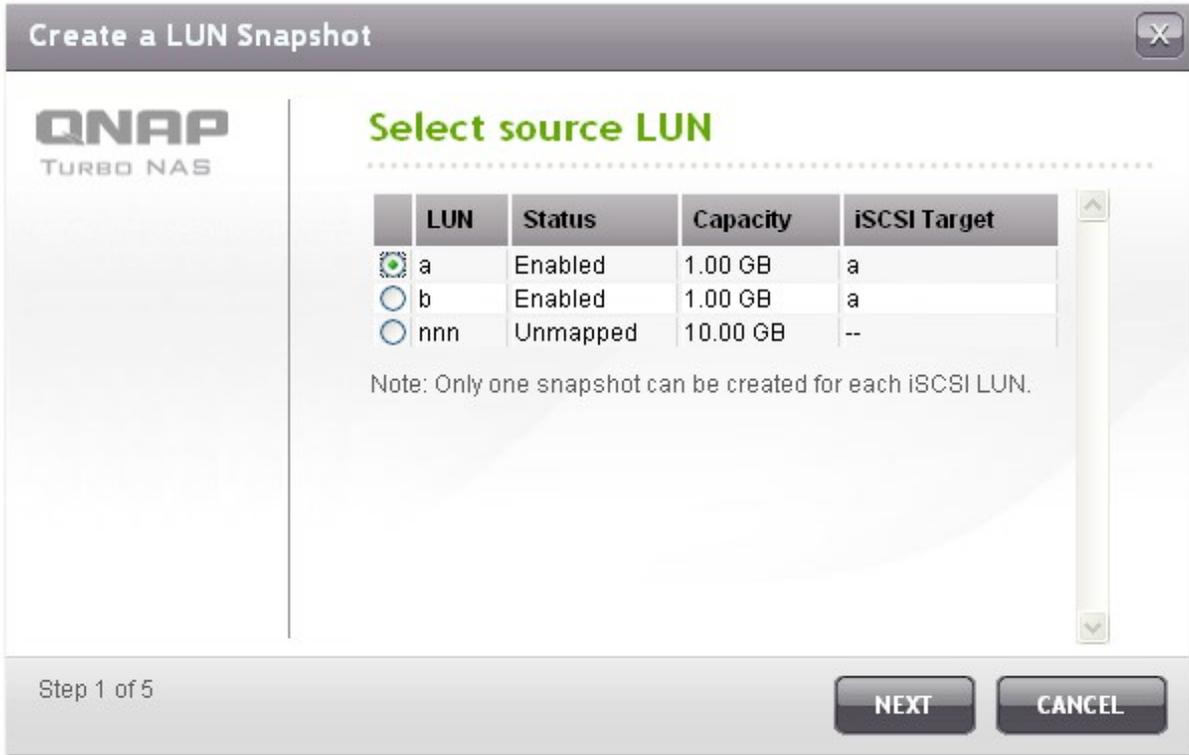
1. To create an iSCSI LUN snapshot, go to "Disk Management" > "iSCSI" > "LUN Backup". Click "Create a new job".



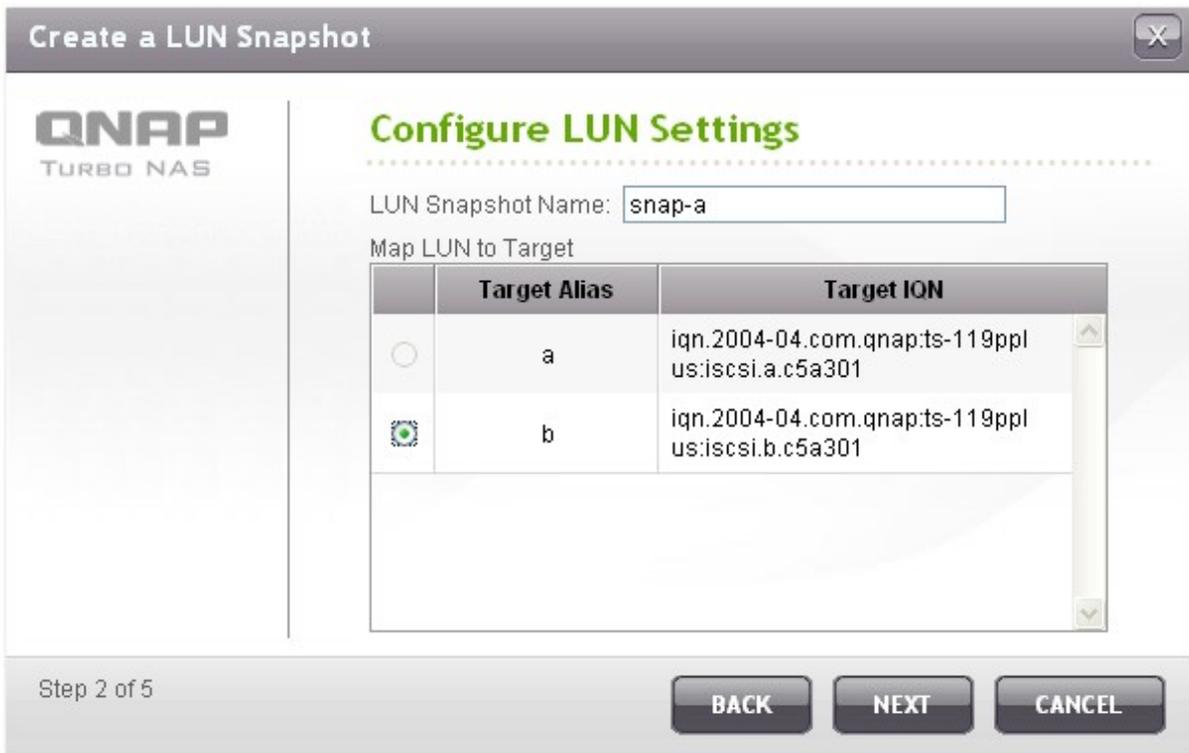
2. Select "Create a LUN Snapshot" and click "Next".



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.

Create a LUN Snapshot

QNAP
TURBO NAS

Snapshot Schedule

Select schedule:
Now

Snapshot duration: -- day(s) 3 hour(s)

Step 3 of 5

BACK NEXT CANCEL

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

Create a LUN Snapshot

QNAP
TURBO NAS

Confirm Settings

Create a LUN Snapshot:

Job Name: Snap_shot-a->snap-a

Source LUN: a (1.00 GB)

LUN Snapshot Name: snap-a

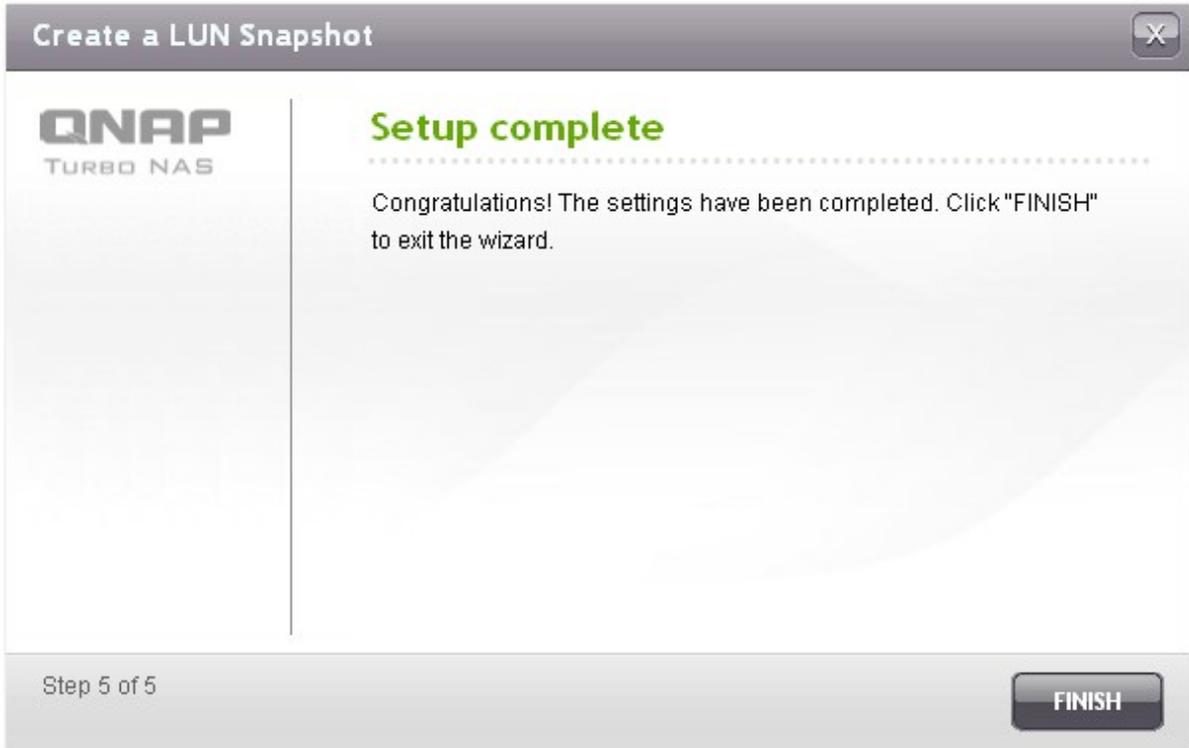
Map LUN to Target: b

Schedule: Now

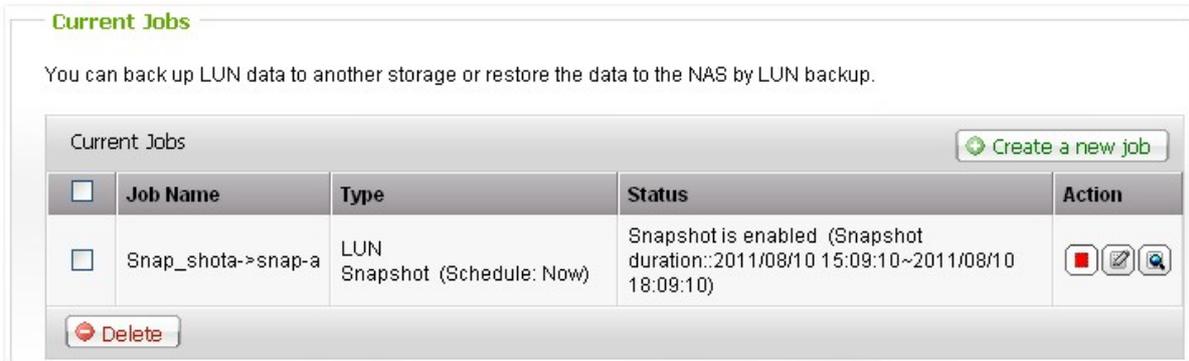
Step 4 of 5

BACK NEXT CANCEL

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.

Target Management

QUICK CONFIGURATION WIZARD Quick Configuration Wizard will assist you to create an iSCSI target and LUN.

iSCSI Target List

+	Alias (IQN)	Status	Action
+	a (iqn.2004-04.com.qnap:ts-119plus:iscsi.a.c5a301)	Ready	⏸️ ✎️ ✖️
-	b (iqn.2004-04.com.qnap:ts-119plus:iscsi.b.c5a301)	Ready	⏸️ ✎️ ✖️
	└ id:0 - snap-a (1.00 GB)	Enabled	⏸️ ✎️

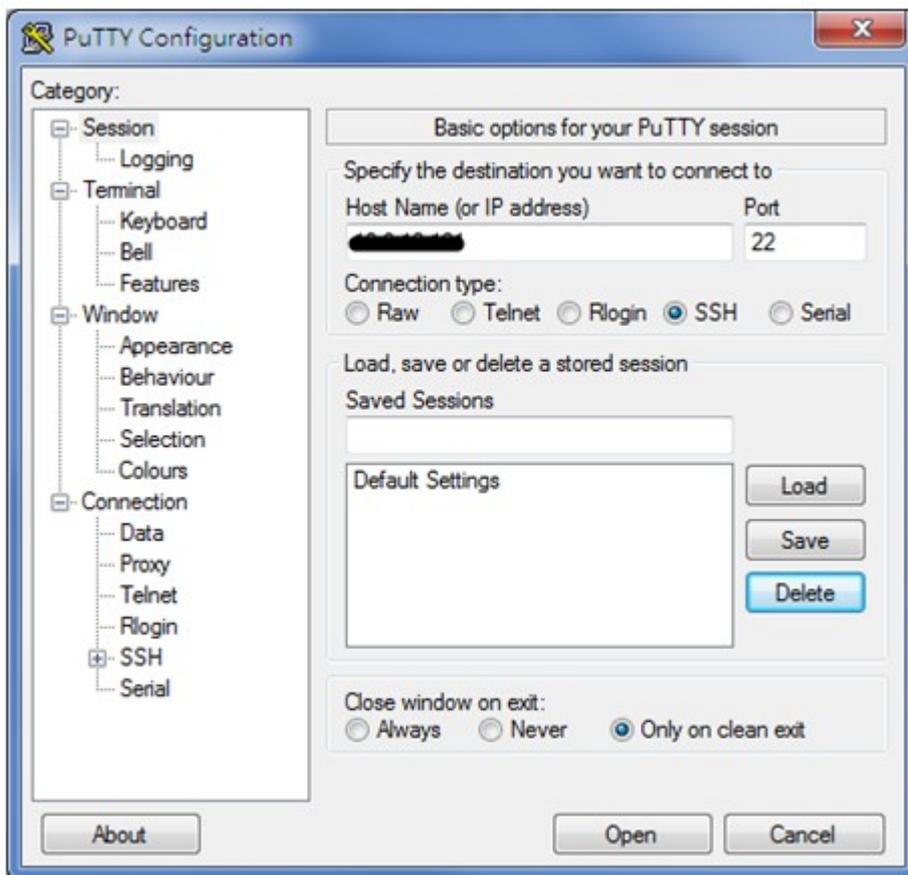
Total: 2 | Display 10 entries per page. 1 / 1

Manage LUN Backup/Restore/Snapshot by Command Line

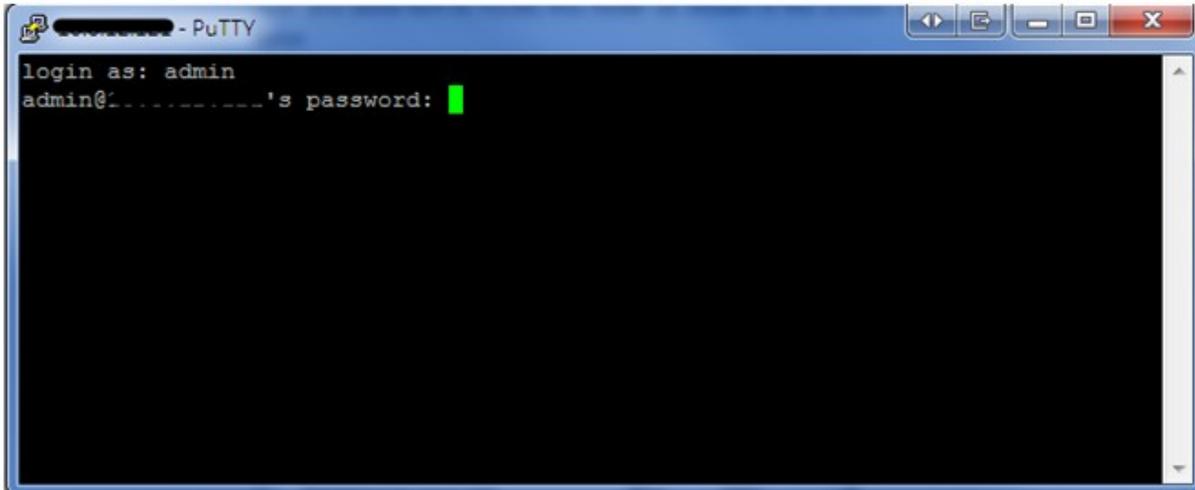
QNAP NAS users can execute or stop the iSCSI LUN backup, restore, or snapshot jobs on the NAS by command line. Follow the instructions below to use this feature.

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.

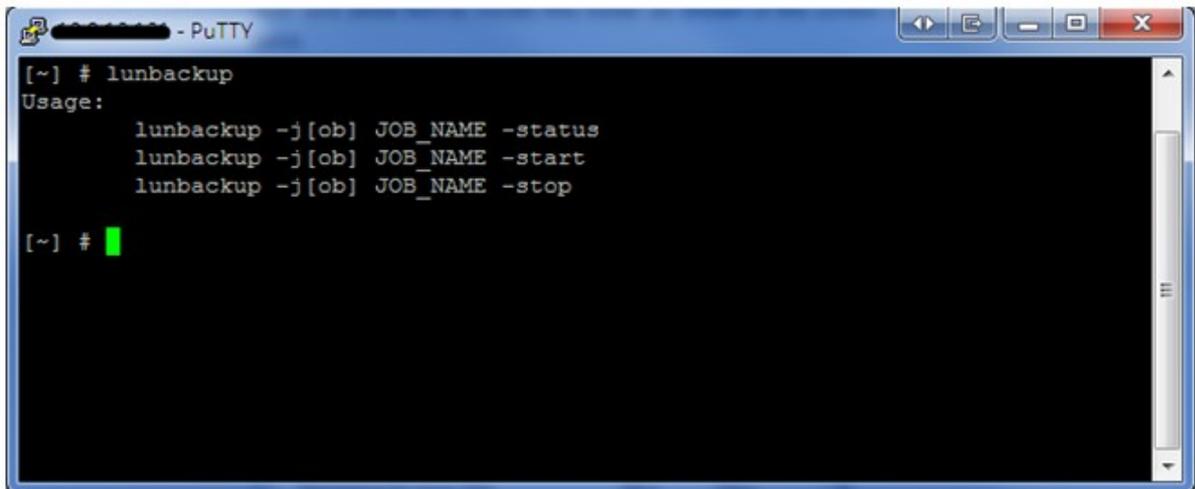


3. Login the NAS as an administrator.



```
login as: admin
admin@'s password: █
```

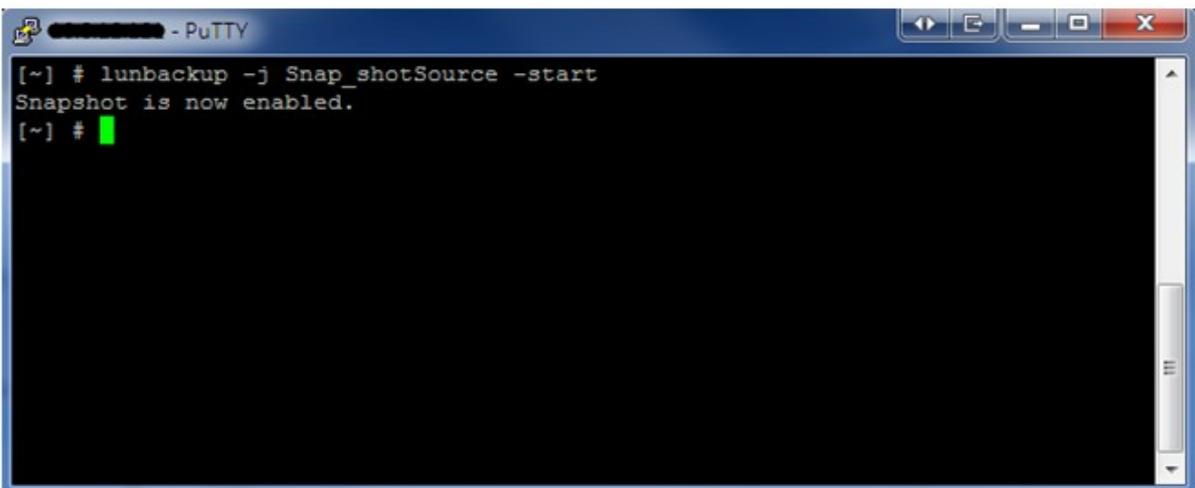
4. Input the command "lunbackup". The command usage description will be shown.



```
[~] # lunbackup
Usage:
    lunbackup -j[ob] JOB_NAME -status
    lunbackup -j[ob] JOB_NAME -start
    lunbackup -j[ob] JOB_NAME -stop

[~] # █
```

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



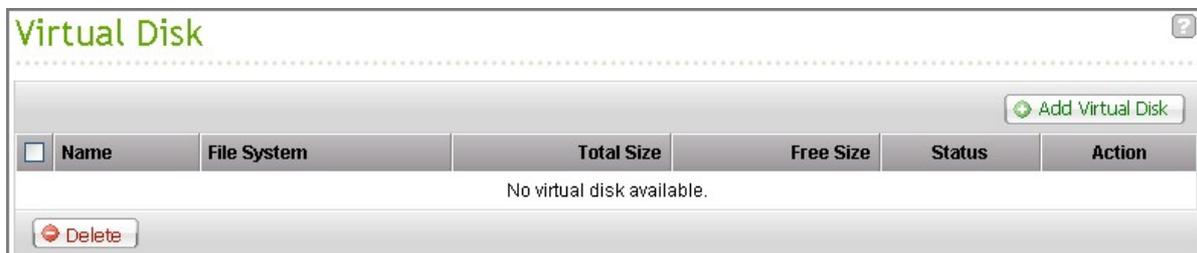
```
[~] # lunbackup -j Snap_shotSource -start
Snapshot is now enabled.
[~] # █
```

4.6 Virtual Disk

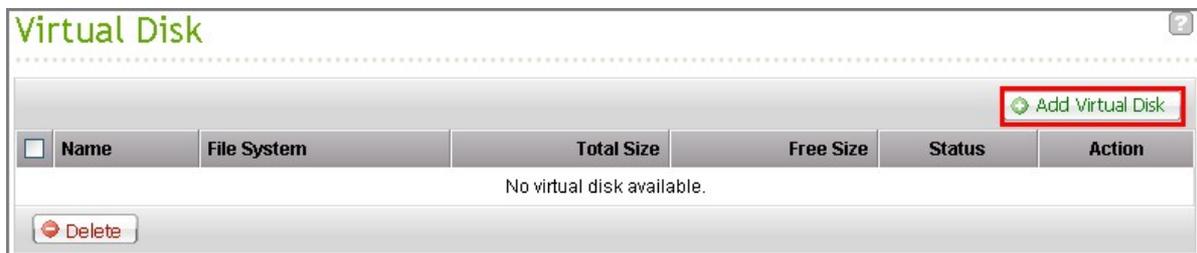
You can use this function to add the iSCSI targets of other QNAP NAS or storage servers to the NAS as the virtual disks for storage capacity expansion. The NAS supports maximum 8 virtual disks.

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 username 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".

Add Virtual Disk

Add Virtual Disk

Target Server IP/Name: 10.8.12.111 Port: 3260

GET REMOTE DISK

Target Name: iqn.2004-04.com.qnap.ts-439proli.iscsi.001.be23f

Initiator IQN: iqn.2004-04.com.qnap.TS-119.QNAPAlex

Authentication

User Name:

Password:

CRC/Checksum (optional)

Data Digest

Header Digest

Step 1 of 3

NEXT **CANCEL**

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.

Add Virtual Disk

Configure Virtual Disk

Virtual Disk Name:

LUN List: File System: ext3

Note: Make sure only this NAS can connect to the selected LUN.

Format virtual disk now

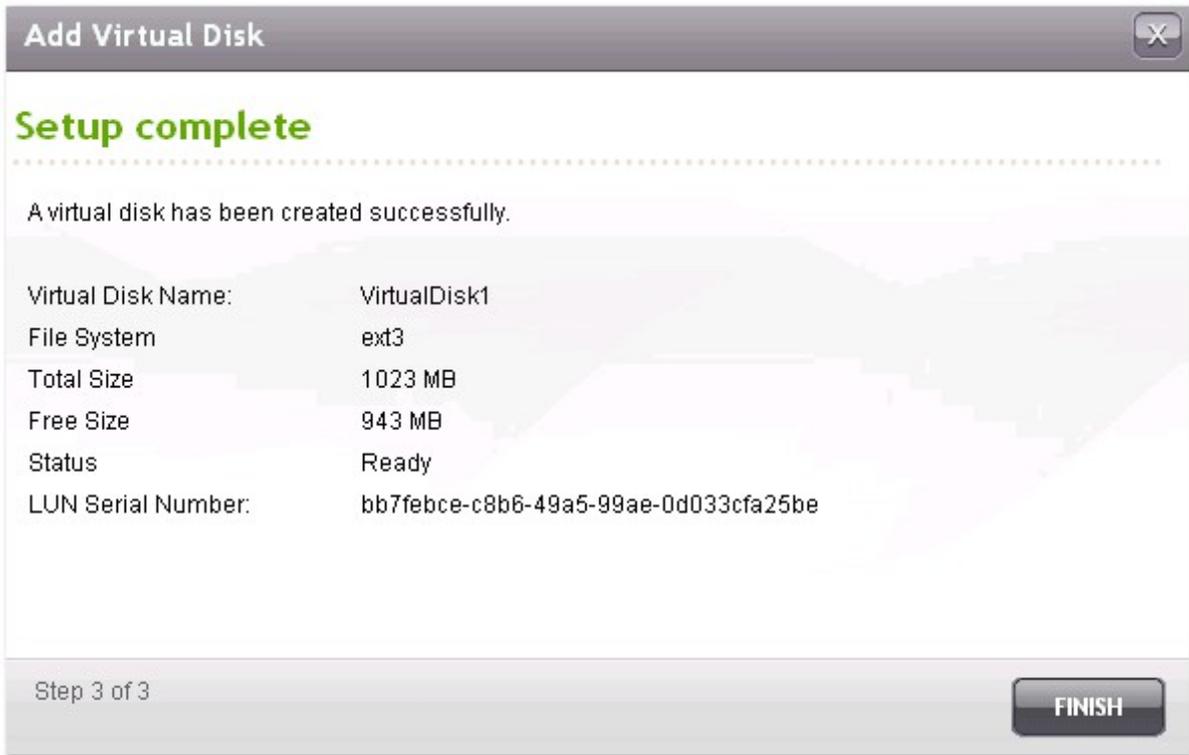
File System

Warning: All the disk data will be removed!

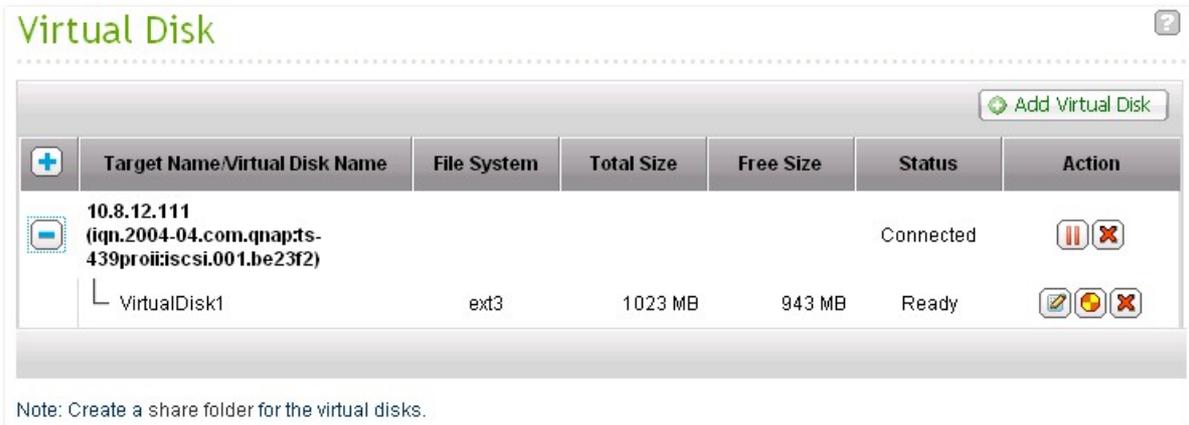
Step 2 of 3

BACK **NEXT** **CANCEL**

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 [\[19\]](#)

Users [\[21\]](#)

User Groups [\[23\]](#)

Share Folders [\[23\]](#)

Quota [\[26\]](#)

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

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 username 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.

The screenshot shows the 'Network' configuration page on a QNAP NAS. The breadcrumb navigation is 'Home >> System Administration >> Network'. The page title is 'Welcome admin | Logout' and the language is 'English'. The 'IP Address' section contains a table with the following data:

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1+2	Yes	10.8.12.46	255.255.254.0	10.8.12.1	00:08:9B:8C:BC:6C	100Mbps	1500		

The 'Default Gateway' section shows 'Use the settings from: Ethernet 1+2'.

The 'Port Trunking' section has 'Enable Network Port Trunking' checked and 'Balance-rr (Round-Robin)' selected.

The 'DNS Server:' section has the 'Primary DNS Server' field highlighted with a red box, containing the IP address 10.8.2.11. The 'Secondary DNS Server' field contains the IP address 10.8.2.9.

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

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

QUICK CONFIGURATION WIZARD Quick Configuration Wizard will help you join the NAS to an Active Directory domain.

Server Description (Optional):	<input type="text" value="myserver"/>
Domain NetBIOS Name:	<input type="text" value="test"/>
AD Server Name:	<input type="text" value="AD"/>
Domain:	<input type="text" value="ADtest.local"/>
Organization Unit (Optional):	<input type="text"/>
Domain Administrator Username:	<input type="text" value="administrator"/>
Domain Administrator Password:	<input type="password" value="••••••"/>

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).

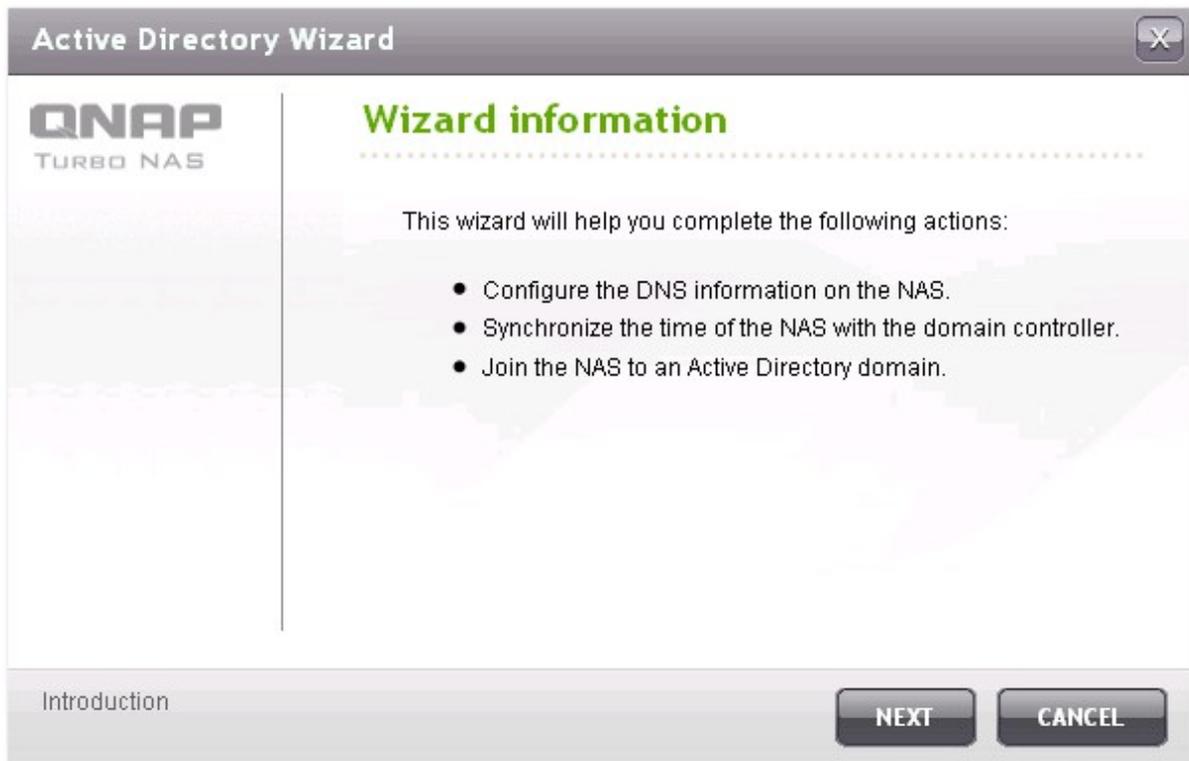
Join the NAS to Active Directory (AD) by Quick Configuration Wizard

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".

The screenshot shows a web interface for "Domain Security" configuration. The breadcrumb trail is "Home >> Access Right Management >> Domain Security". The user is logged in as "admin" and the language is set to "English". The page title is "Domain Security". Under the heading "Domain Security for File Services", there are three radio button options: "No domain security (local users only)", "Active Directory authentication (domain member)", and "LDAP authentication". The "Active Directory authentication (domain member)" option is selected and highlighted with a red box. Below this, there is a "QUICK CONFIGURATION WIZARD" button, also highlighted with a red box, followed by the text: "Quick Configuration Wizard will help you join the NAS to an Active Directory domain." Below this text are seven input fields for configuration: "Server Description (Optional)", "Domain NetBIOS Name", "AD Server Name", "Domain", "Organization Unit (Optional)", "Domain Administrator Username", and "Domain Administrator Password". An "APPLY" button is located at the bottom right of the form.

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".

QNAP
TURBO NAS

Domain name service (DNS) and Domain information

Full DNS domain name:
Example: mydomain.local

NetBios domain name:
Example: MYDOMAIN

Enter the DNS Server IP for the domain resolution. It must be the DNS server of your Active Directory.

Obtain DNS server address automatically by DHCP server.

Domain DNS Server: . . .

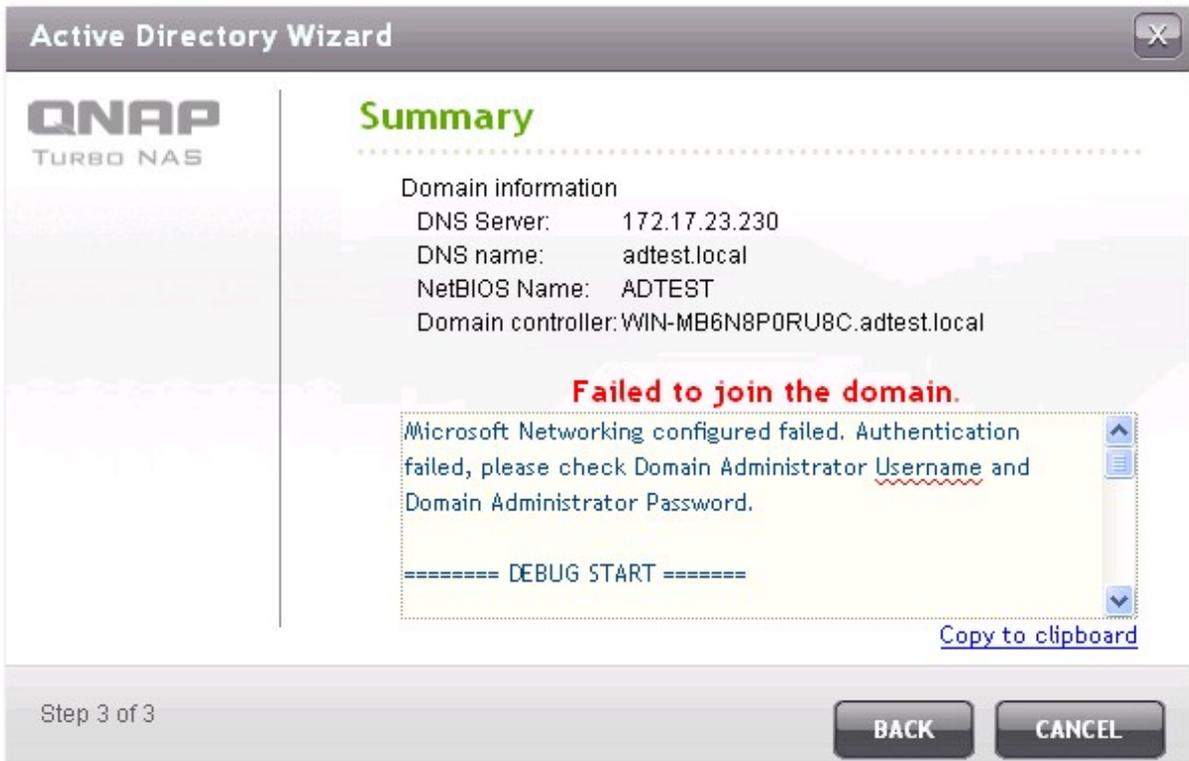
Step 1 of 3

BACK **NEXT** **CANCEL**

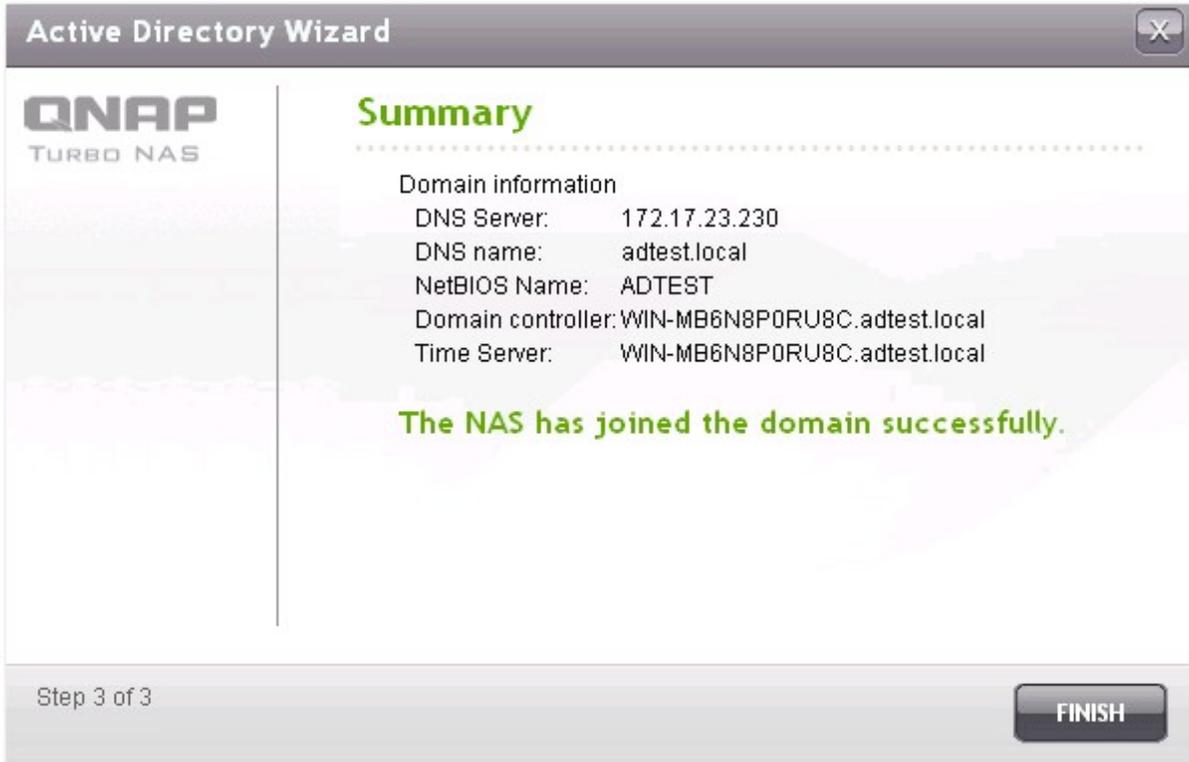
4. Select a domain controller from the drop-down menu. The domain controller is responsible for time synchronization between the NAS and the domain server and user authentication. Enter the domain administrator name and password. Click "JOIN".



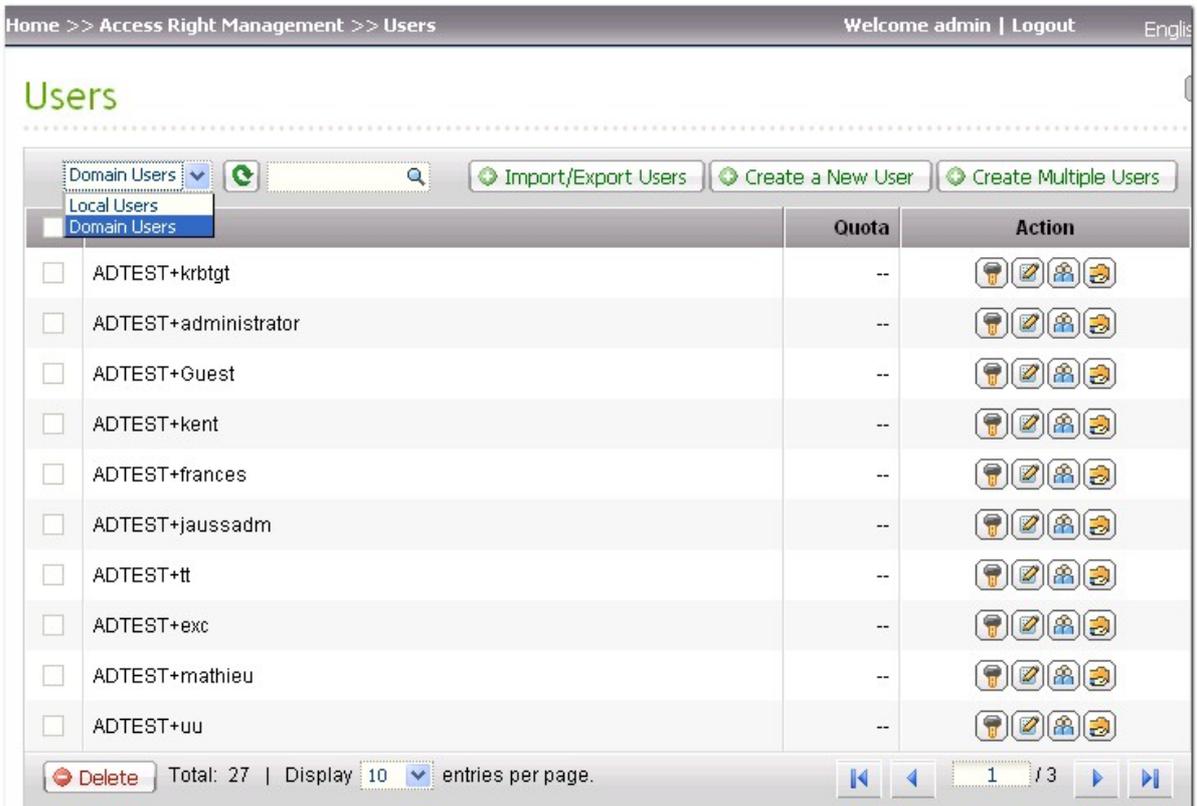
5. If you failed to join the NAS to the domain, you could copy the error logs or go back to modify the settings.



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

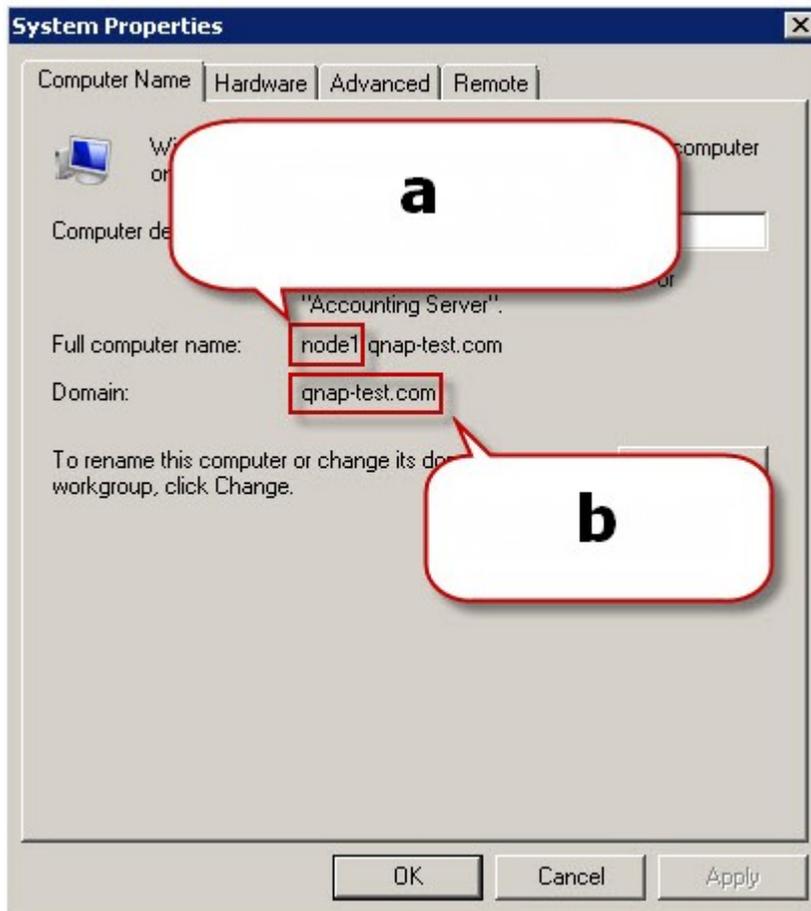


- Go to "Access Right Management" > "Users" or "User Groups" to load the domain users or user groups to the NAS.



Windows 2003

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



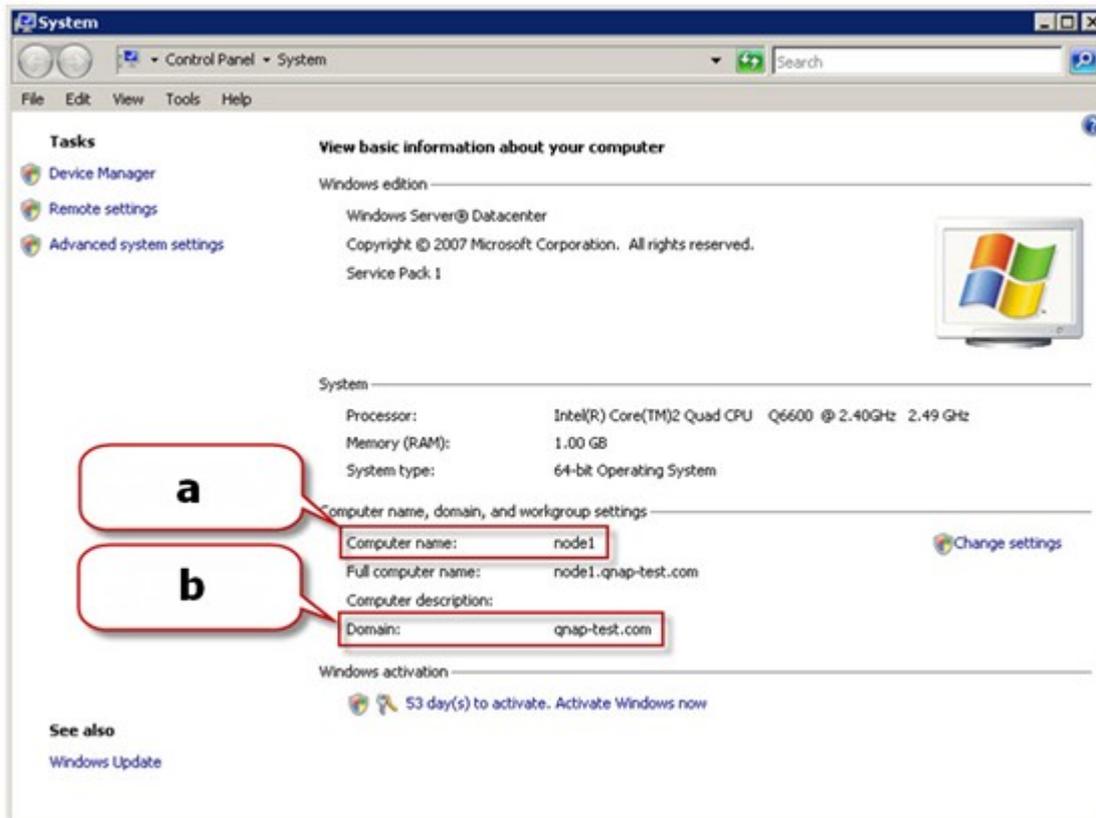
- a. In Windows 2003 servers, the AD server name is "node1" NOT "node1.qnap-test.com".
- b. The domain name remains the same.

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.



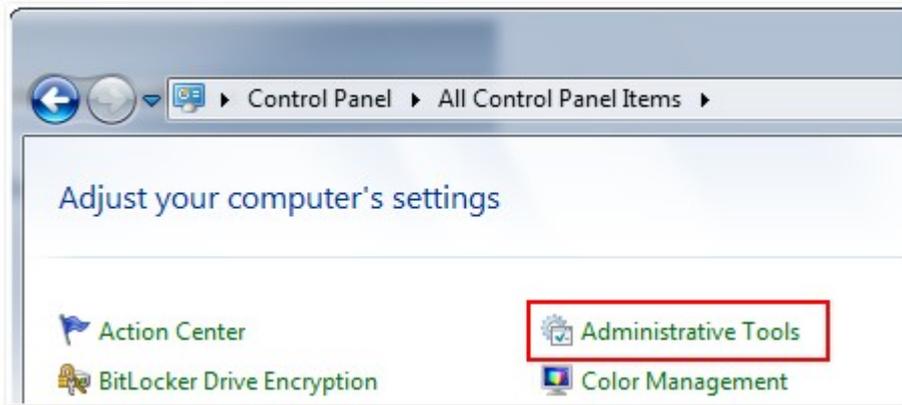
Note:

- 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 usernames 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.

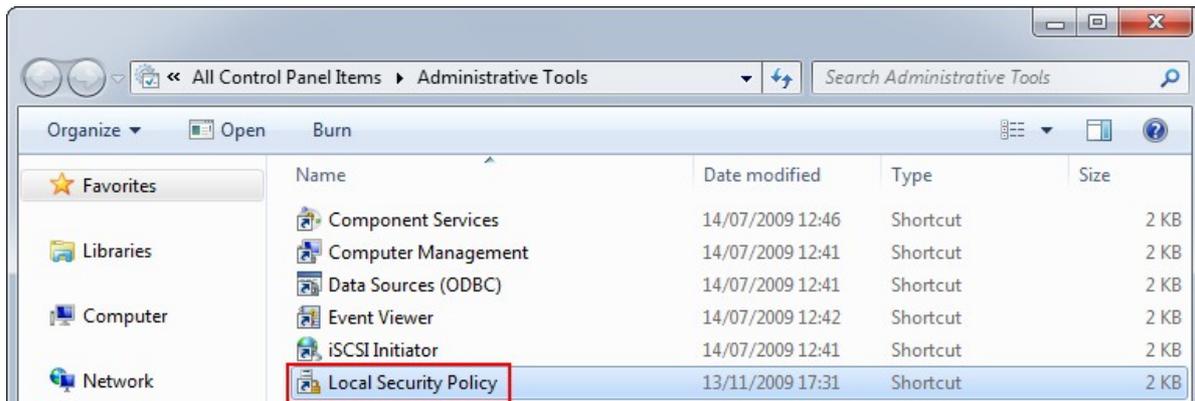
Windows 7

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.

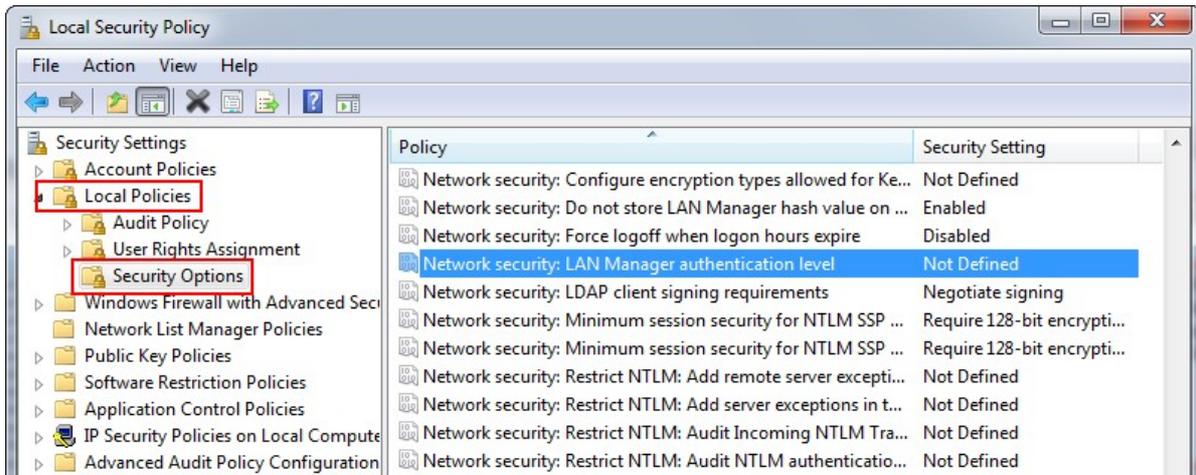
- a. Go to "Control Panel" > "Administrative Tools".



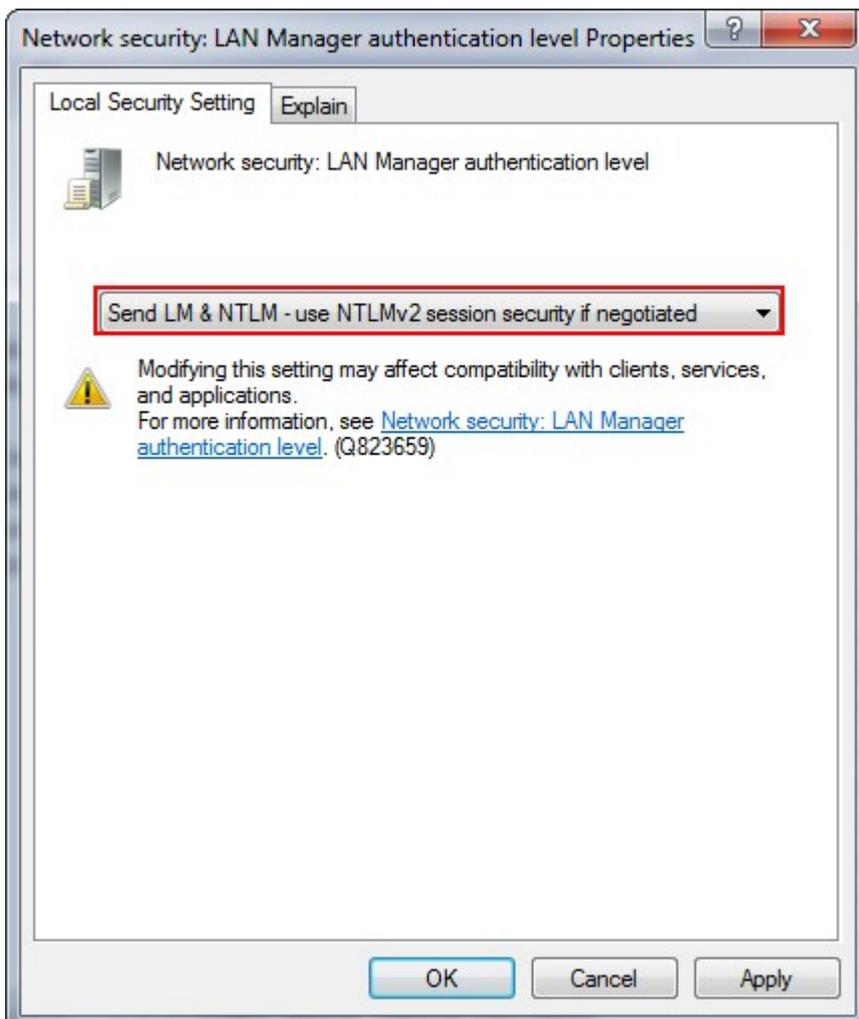
- b. Click "Local Security Policy".



- 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.

Domain Security

Domain Security for File Services

No domain security (local users only)

Active Directory authentication (domain member)

LDAP authentication

Select the type of LDAP server: Remote LDAP Server

Status: Offline

LDAP Server Host: 10.8.13.59

LDAP Security: ldap://

BASE DN: dc=my-domain,dc=local

Root DN: cn=admin,dc=my-domain,dc=local

Password:

Users Base DN: ou=people,dc=my-domain,dc=local

Group Base DN: ou=group,dc=my-domain,dc=local

You can enable LDAP authentication for Microsoft Networking ([Samba](#))

Current Samba ID: S-1-5-21-1496176302-4157969542-1351159741

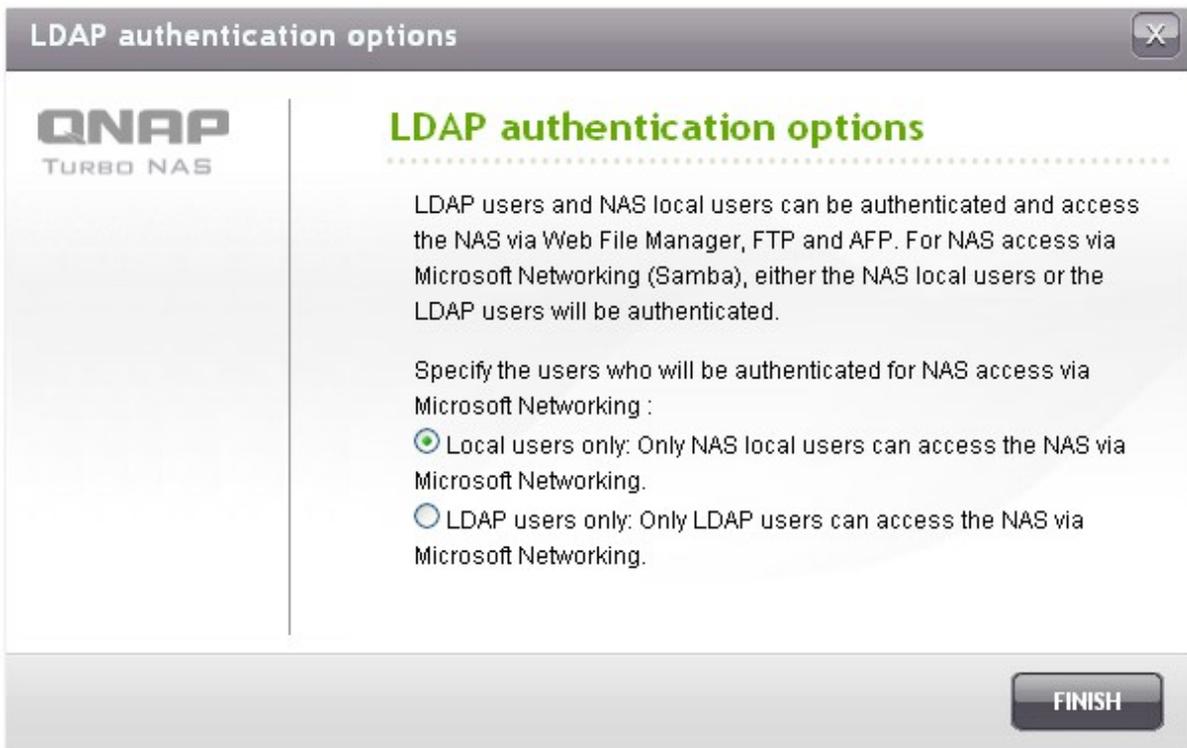
APPLY

- 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.

The screenshot shows a web interface for configuring Microsoft Networking. At the top, there is a breadcrumb trail: Home >> Network Services >> Microsoft Networking. On the right, it says 'Welcome admin | Logout' and 'English'. The main heading is 'Microsoft Networking'. Below this, there are two tabs: 'MICROSOFT NETWORKING' (selected) and 'ADVANCED OPTIONS'. The 'MICROSOFT NETWORKING' section contains the following options:

- Enable file service for Microsoft networking
 - Server Description (Optional):
 - Workgroup:
 - Standalone Server
 - AD Domain Member (To enable Domain Security, please click here.)
 - LDAP Domain Authentication (To enable Domain Security, please click here.)

At the bottom of the section, it displays 'Current Samba ID S-1-5-21-325120726-1639715159-2191483818'. An 'APPLY' button is located at the bottom right of the configuration area.

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" .

Home >> Access Right Management >> Share Folders Welcome admin | Logout English

Share Folders

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Shares New Share Folder Restore Default Network Shares

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Network Recycle Bin 1	4 KB	0	0	No	  NFS   
<input type="checkbox"/>	Public	25.04 GB	48	710	No	  NFS   

Select users and groups

Domain Users  Total: 4 1 / 1

Name	Read only	Read/Write	Deny Access
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ADD CANCEL

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=qnab,dc=com

Root DN: cn=admin,dc=qnab,dc=com

Users Base DN: ou=people,dc=qnab,dc=com

Groups Base DN: ou=group,dc=qnab,dc=com

2. Mac Open Directory Server

Base DN: dc=macserver,dc=qnab,dc=com

Root DN: uid=root,cn=users,dc=macserver,dc=qnab,dc=com

Users Base DN: cn=users,dc=macserver,dc=qnab,dc=com

Groups Base DN: cn=groups,dc=macserver,dc=qnab,dc=com

5.2 Users

The NAS has created the following users by default:

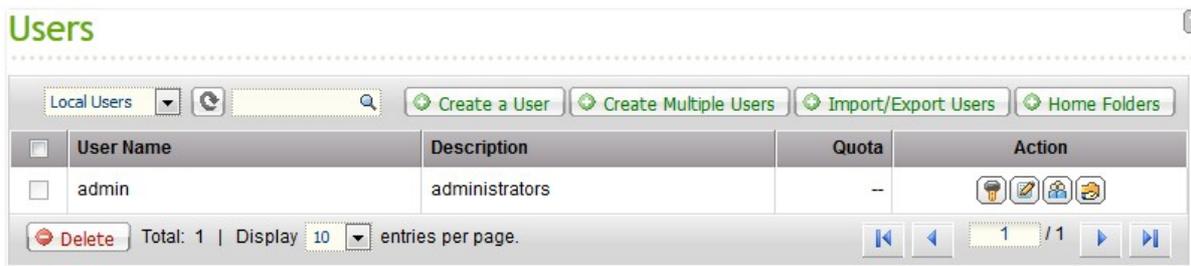
- admin
The administrator "admin" has full access to system administration and all network shares. It cannot be deleted.
- guest
This is a built-in user and will not be displayed on the "User Management" page. A guest does not belong to any user group. The login password is "guest".
- anonymous
This 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:

- Username
The username is case-insensitive and supports multi-byte characters, such as Chinese, Japanese, Korean, and Russian. The maximum length is 32 characters. 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.

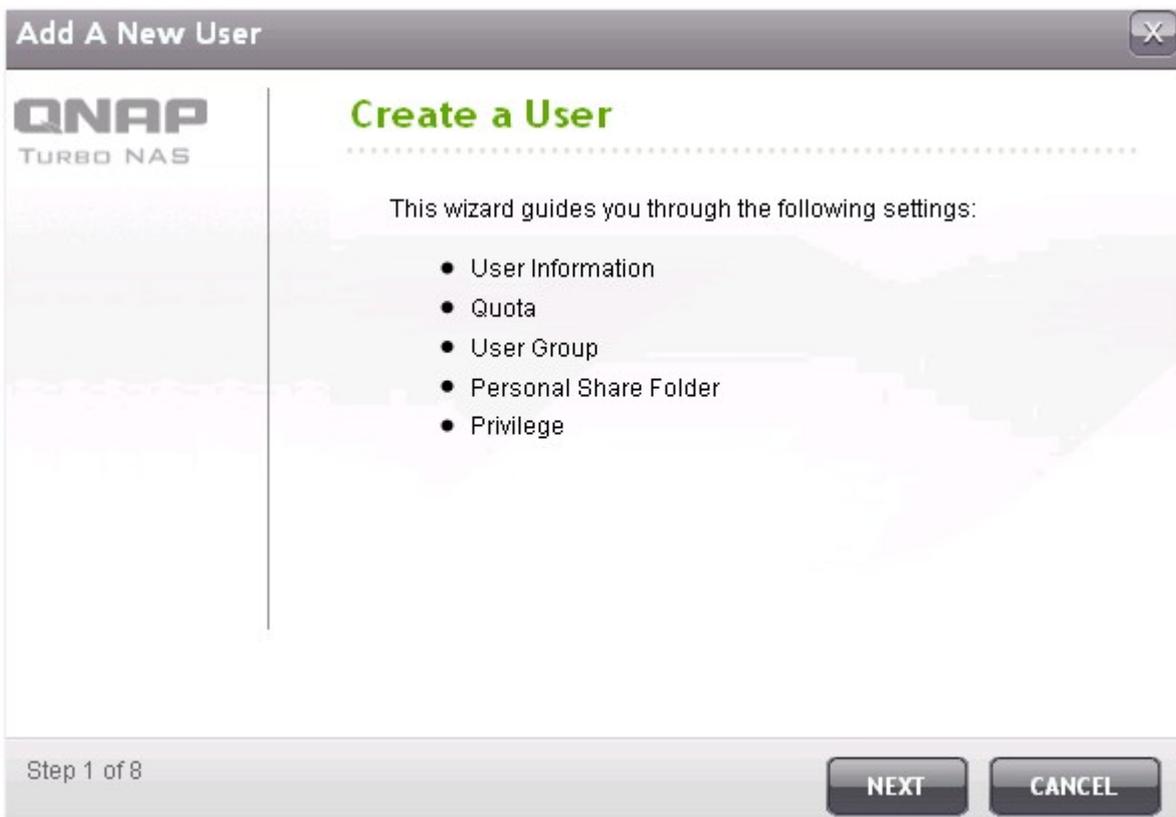


Create a User

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

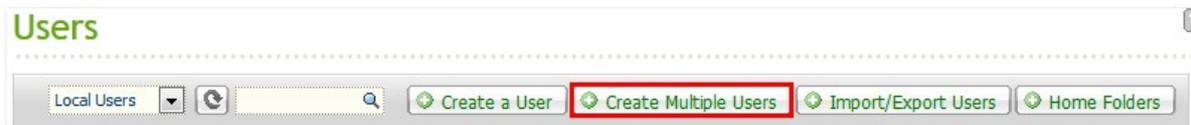


Follow the instructions of the wizard to complete the details.



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 username, 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.

Multiple Users Creation Wizard

QNAP
TURBO NAS

Account Login Info

User Name Prefix :

User Name Start No :

Number of Users :

Password :

Verify Password :

Note: For increased security, password should be at least 6 characters.

Step 2 of 5

BACK **NEXT** **CANCEL**

4. Select to create a private network share for each user or not. The network share will be named after the username. 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.

Users

Local Users

<input type="checkbox"/>	User Name	Quota	Action
<input type="checkbox"/>	admin	--	
<input type="checkbox"/>	test0001	1000 MB	
<input type="checkbox"/>	test0002	1000 MB	
<input type="checkbox"/>	test0003	1000 MB	
<input type="checkbox"/>	test0004	1000 MB	
<input type="checkbox"/>	test0005	1000 MB	
<input type="checkbox"/>	test0006	1000 MB	
<input type="checkbox"/>	test0007	1000 MB	
<input type="checkbox"/>	test0008	1000 MB	
<input type="checkbox"/>	test0009	1000 MB	

Total: 11 | Display 10 entries per page. 1 / 2

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

Home >> Access Right Management >> Share Folders Welcome admin | Logout English

Share Folders ?

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Shares

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	test0001	4 KB	0	0	No	
<input type="checkbox"/>	test0002	4 KB	0	0	No	
<input type="checkbox"/>	test0003	4 KB	0	0	No	
<input type="checkbox"/>	test0004	4 KB	0	0	No	
<input type="checkbox"/>	test0005	4 KB	0	0	No	
<input type="checkbox"/>	test0006	4 KB	0	0	No	
<input type="checkbox"/>	test0007	4 KB	0	0	No	
<input type="checkbox"/>	test0008	4 KB	0	0	No	
<input type="checkbox"/>	test0009	4 KB	0	0	No	
<input type="checkbox"/>	test0010	4 KB	0	0	No	

Total: 20 | Display entries per page. 2 / 2

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".

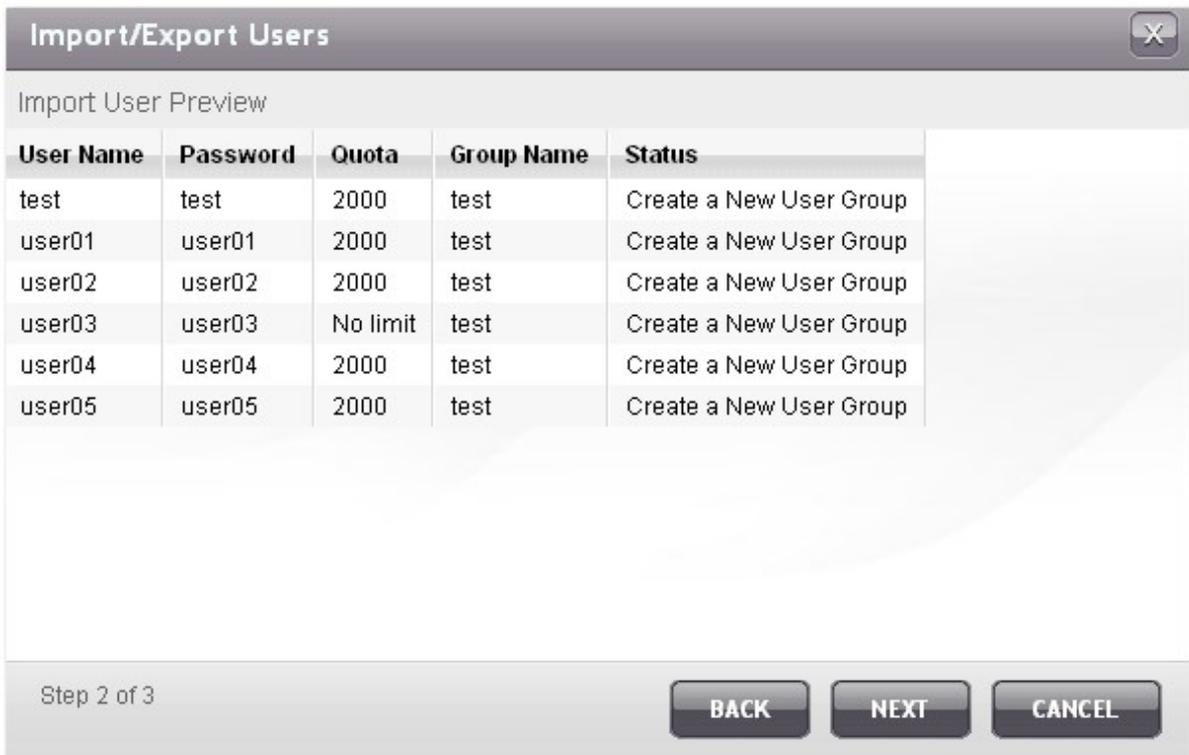


2. Select "Import user and user group settings". Select the option "Overwrite duplicate users" to overwrite existing users on the NAS.



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.

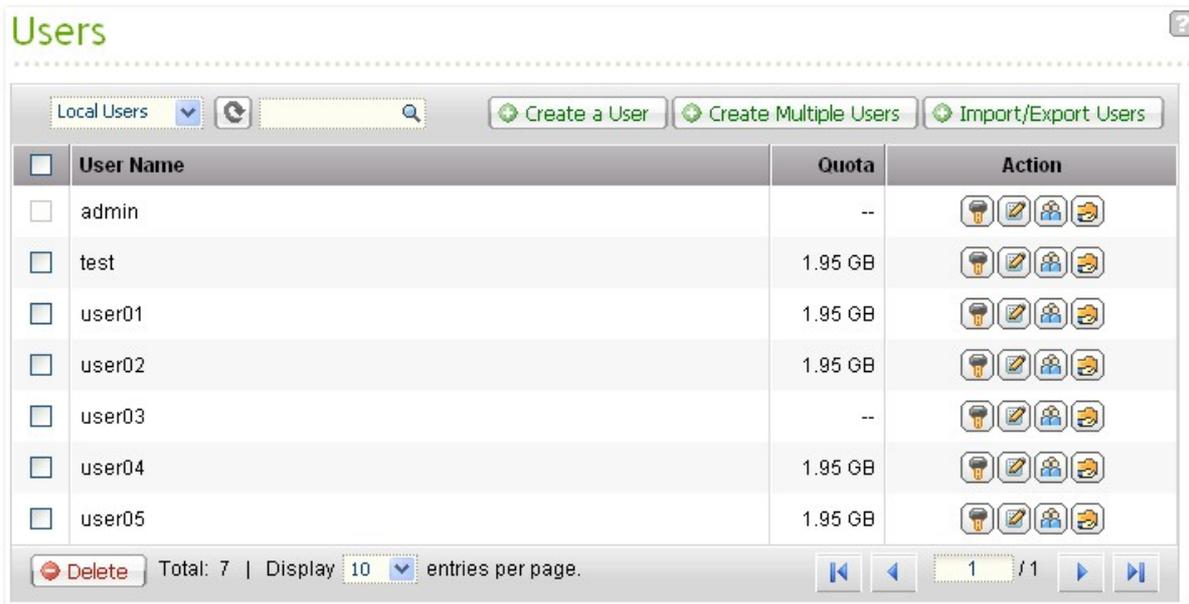


5. Click "Next" to create the user accounts.

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



7. The imported user accounts will be shown.

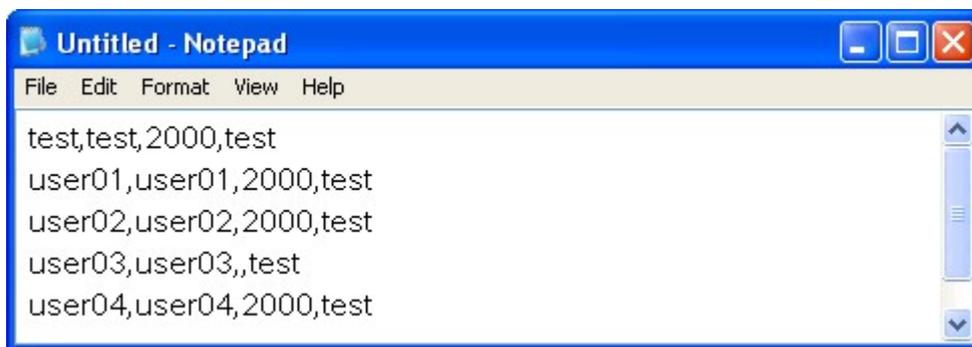


The NAS supports importing user accounts from TXT, CSV or BIN files. To create a list of user accounts with these file types, follow the steps below.

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

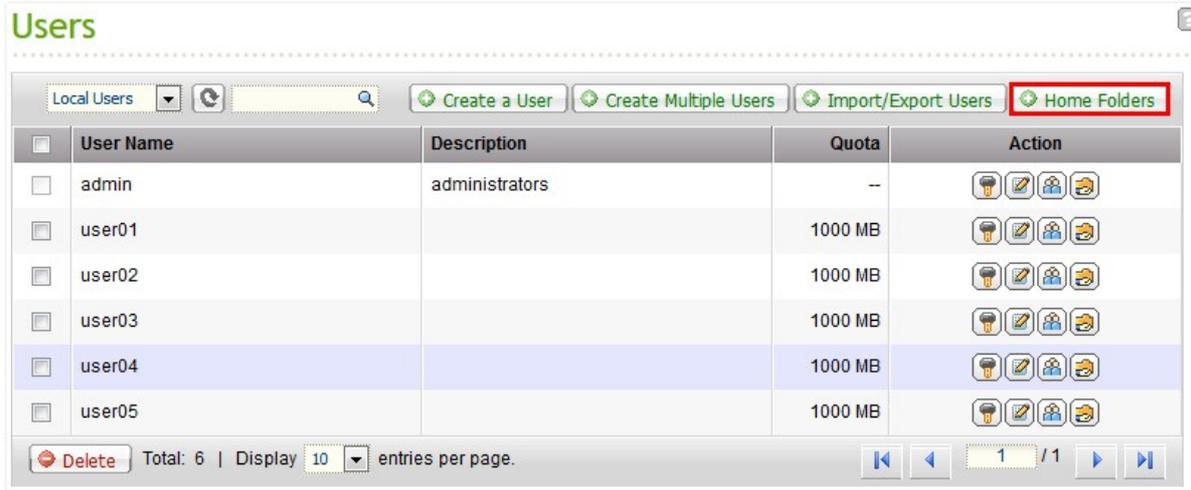
BIN (Exported from the NAS)

The BIN file is exported from a QNAP NAS. It contains information including username, 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.

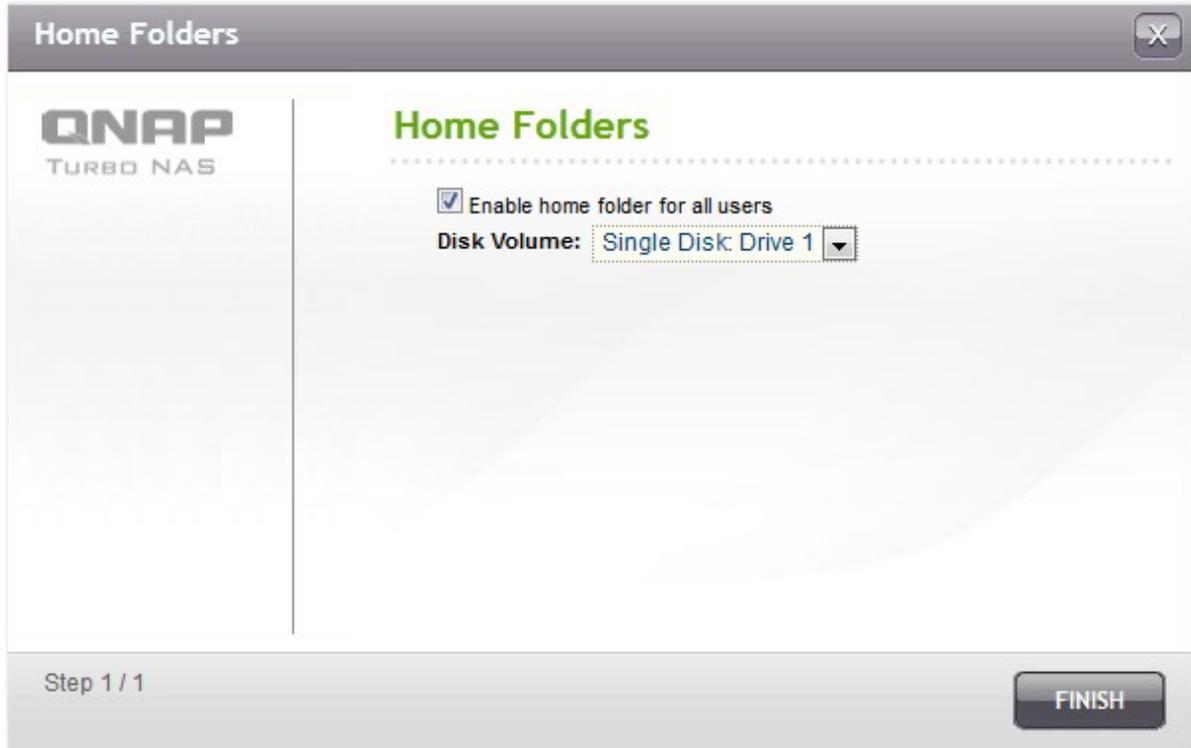
To use this feature, click "Home Folders".



The screenshot shows the 'Users' management page. At the top, there are buttons for 'Local Users', 'Create a User', 'Create Multiple Users', 'Import/Export Users', and 'Home Folders'. The 'Home Folders' button is highlighted with a red border. Below the buttons is a table with columns: 'User Name', 'Description', 'Quota', and 'Action'. The table lists users: 'admin' (description: administrators, quota: --), 'user01', 'user02', 'user03', 'user04', and 'user05' (all with quota: 1000 MB). The 'Action' column contains icons for adding, editing, deleting, and sharing. At the bottom, there is a 'Delete' button, a status bar showing 'Total: 6 | Display 10 entries per page.', and navigation arrows.

<input type="checkbox"/>	User Name	Description	Quota	Action
<input type="checkbox"/>	admin	administrators	--	   
<input type="checkbox"/>	user01		1000 MB	   
<input type="checkbox"/>	user02		1000 MB	   
<input type="checkbox"/>	user03		1000 MB	   
<input type="checkbox"/>	user04		1000 MB	   
<input type="checkbox"/>	user05		1000 MB	   

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



The screenshot shows the 'Home Folders' configuration window. The window title is 'Home Folders'. On the left, there is the QNAP TURBO NAS logo. The main content area has the title 'Home Folders' and a checkbox labeled 'Enable home folder for all users' which is checked. Below it, there is a 'Disk Volume:' label followed by a dropdown menu showing 'Single Disk: Drive 1'. At the bottom left, it says 'Step 1 / 1'. At the bottom right, there is a 'FINISH' button.

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).

The screenshot displays the 'Share Folders' management page. At the top, there are navigation tabs: 'SHARE FOLDERS' (selected), 'ISO SHARE FOLDERS', 'FOLDER AGGREGATION', and 'ADVANCED OPTIONS'. Below the tabs is a search bar and two buttons: 'New Share Folder' and 'Restore Default Network Shares'. The main content is a table listing shares:

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Dept	80 KB	17	2	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Download	400.2 MB	7	8	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Multimedia	12.84 GB	65	575	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Network Recycle Bin 1	120.13 MB	22	27	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Public	26.55 GB	319	1650	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Recordings	88 KB	19	2	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Usb	28 KB	4	2	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input type="checkbox"/>	Web	236.48 MB	263	2108	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input checked="" type="checkbox"/>	aaa	4 KB	0	0	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]
<input checked="" type="checkbox"/>	ivan	4.7 MB	0	1	No	[Edit] [Share] [NFS] [SMB] [FTP] [Recycle]

At the bottom of the table, there is a 'Delete' button, a summary 'Total: 12 | Display 10 entries per page.', and pagination controls showing '1 / 2'.

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

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Download	29.58 MB	28	33	No	
<input type="checkbox"/>	Multimedia	19.87 GB	346	3994	No	
<input type="checkbox"/>	Network Recycle Bin 1	13.45 KB	4	2	No	
<input type="checkbox"/>	Public	5.49 GB	1446	16459	No	
<input type="checkbox"/>	Recordings	25.45 KB	19	2	No	
<input type="checkbox"/>	Usb	13.45 KB	4	2	No	
<input type="checkbox"/>	Web	21.06 MB	86	1076	No	
<input checked="" type="checkbox"/>	root	170.08 GB	2973	64813	No	

Shares

Total: 8 | Display entries per page. 1 / 1

2. Click "Next".

QNAP
TURBO NAS

Create a Share Folder

This wizard guides you through the following settings:

- Share Folder Settings
- Privilege

To continue, click **Next**. To exit, click **Cancel**.

Step 1 of 7

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.

The screenshot shows a dialog box titled "Create A Share Folder" with a close button in the top right corner. On the left side, there is a logo for "QNAP TURBO NAS". The main area is titled "Share Folder Settings" and contains the following fields and options:

- Folder Name:** A text input field containing "test" with a green checkmark icon to its right.
- Disk Volume:** A dropdown menu showing "Mirroring Disk Volume: Drive 1 2".
- Hide Folder:** Radio buttons for "Yes" and "No", with "No" selected and a green information icon to its right.
- Lock file (oplocks):** Radio buttons for "Yes" and "No", with "Yes" selected.
- Path:** Radio buttons for "Specify path automatically" and "Enter path manually", with "Specify path automatically" selected.
- Description:** A text input field.

At the bottom left, it says "Step 2 of 7". At the bottom right, there are three buttons: "BACK", "NEXT", and "CANCEL".

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

QNAP
TURBO NAS

Privilege

You can select one of the following methods to configure the user access right to the network share folder:

- Full access (Grant full access right for everyone)
- By User
- By User Group
- Only the system administrator (admin) has full access. General users have **Read Only** access.

Guest Access Right:

- Deny Access
- Read only
- Read/Write

Step 3 of 7

BACK NEXT CANCEL

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.

Create A Share Folder [X]

Access Control (By User)

Search: Total: 7 [1] / 1

User Name	Read only	Read/Write	Deny Access
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
user02	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
user03	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
user04	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
user05	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Step 4 of 7

BACK NEXT CANCEL

6. Confirm the settings and click "Next".

Create A Share Folder

QNAP
TURBO NAS

Confirm Settings

Folder Name: test
Hide Folder: No
Lock file (oplocks): Yes
Path: Mirroring Disk Volume: Drive 1 2 /test
Description: ---
Access right: By User
Access User/User Group: admin, test, user02, user03, user04, user05 ...

Step 6 of 7

BACK NEXT CANCEL

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.

The screenshot shows the 'Share Folders' management interface. A confirmation dialog is displayed over a table of shares. The dialog asks: 'All the selected share folder(s) will be removed. Are you sure?' with an option to 'Also delete the data in these folder(s)'. The 'Delete' button in the bottom left of the interface is highlighted with a red box.

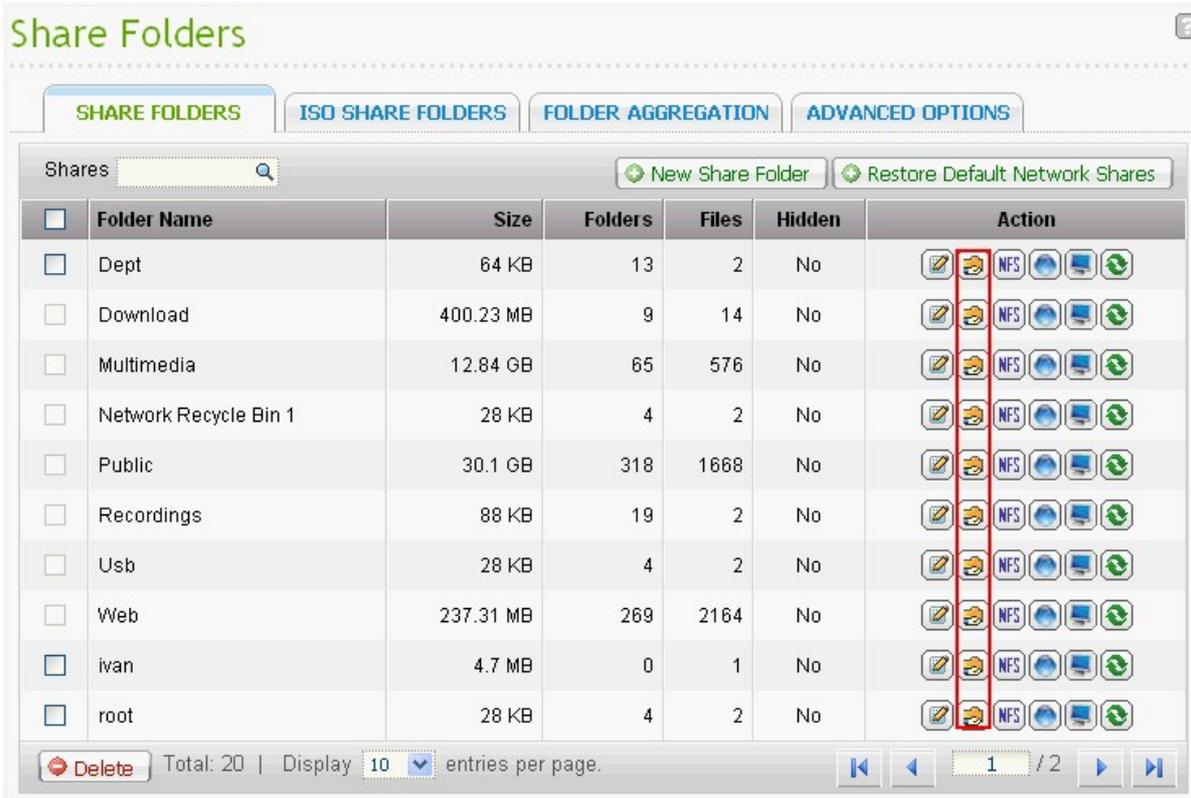
Share Name	Size	Files	Hidden	Action
Public	26.55 GB	319	1650	No
Recordings	88 KB	19	2	No
Usb	28 KB	4	2	No
Web	236.48 MB	263	2108	No
aaa	4 KB	0	0	No
ivan	4.7 MB	0	1	No

At the bottom of the interface, it shows: Total: 12 | Display 10 entries per page. Page 1 / 2.

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 .



Share Folders

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Shares

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Dept	64 KB	13	2	No	NFS
<input type="checkbox"/>	Download	400.23 MB	9	14	No	NFS
<input type="checkbox"/>	Multimedia	12.84 GB	65	576	No	NFS
<input type="checkbox"/>	Network Recycle Bin 1	28 KB	4	2	No	NFS
<input type="checkbox"/>	Public	30.1 GB	318	1668	No	NFS
<input type="checkbox"/>	Recordings	88 KB	19	2	No	NFS
<input type="checkbox"/>	Usb	28 KB	4	2	No	NFS
<input type="checkbox"/>	Web	237.31 MB	269	2164	No	NFS
<input checked="" type="checkbox"/>	ivan	4.7 MB	0	1	No	NFS
<input checked="" type="checkbox"/>	root	28 KB	4	2	No	NFS

Total: 20 | Display entries per page. / 2

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.

Share Folders

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Folder Name:	Permission:	Read only	Read/Write	Deny Access
Dept	everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

+ Add - Remove

Guest Access Right: Deny access

For detailed instructions, please [click here](#)

APPLY

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

Name	Read only	Read/Write	Deny Access
messagebus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
alex	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ivan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
icecast	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test0002	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test0003	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test0004	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test0005	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test0006	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

Share Folders

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Folder Name:	Permission:	Read only	Read/Write	Deny Access
Dept	everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	test0002	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	test0003	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	test0004	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

+ Add - Remove

Guest Access Right: Deny access

For detailed instructions, please [click here](#)

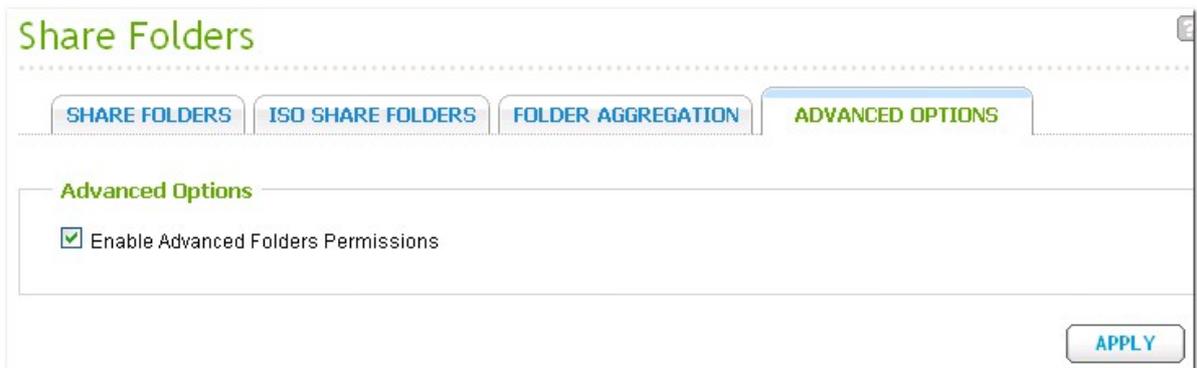
APPLY

Subfolder Permissions

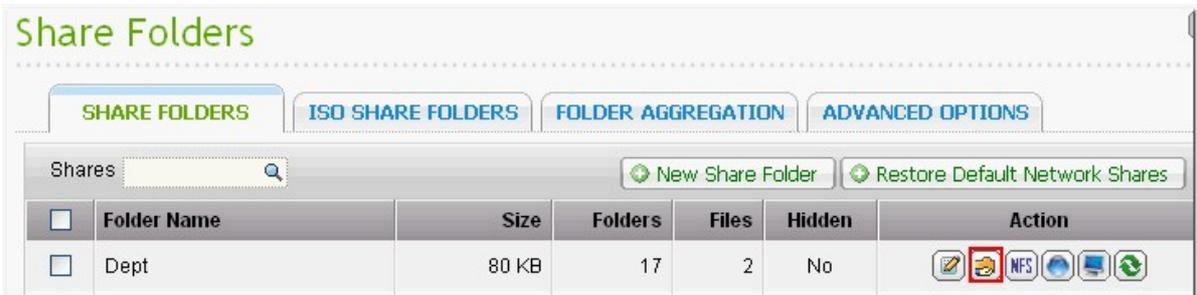
The NAS supports subfolder permissions for secure management of the folders and subfolders. You can specify read, read/write, and deny access of individual user to each folder and subfolder.

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

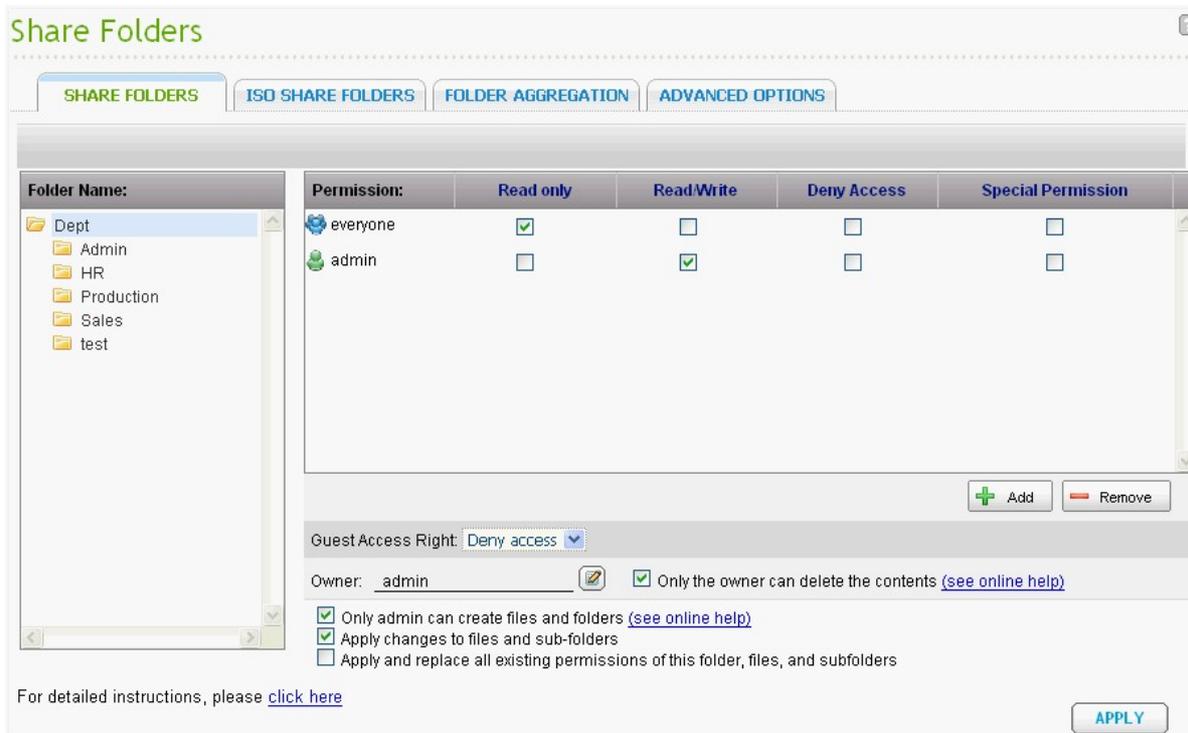
Note: You can create maximum 230 permission entries for each folder when Advanced Folder Permission is enabled.



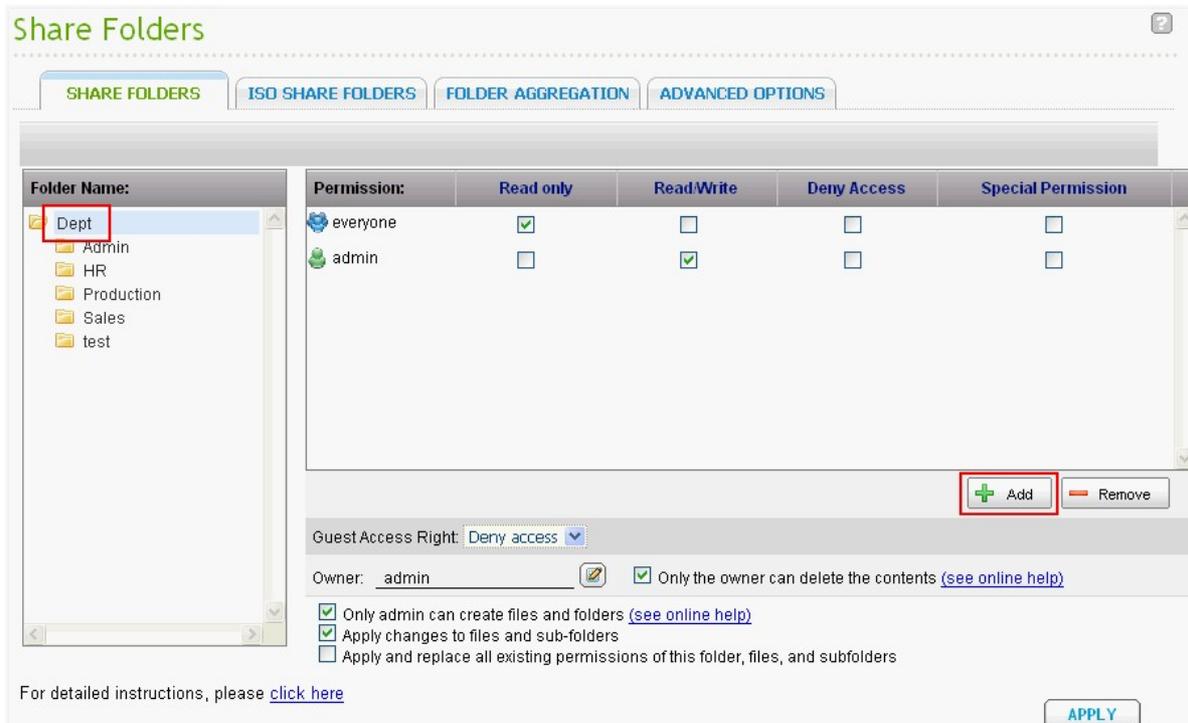
Go to "Access Right Management" > "Share Folders" > "Share Folders" tab. Select a root folder, for example Dept, and click .



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.



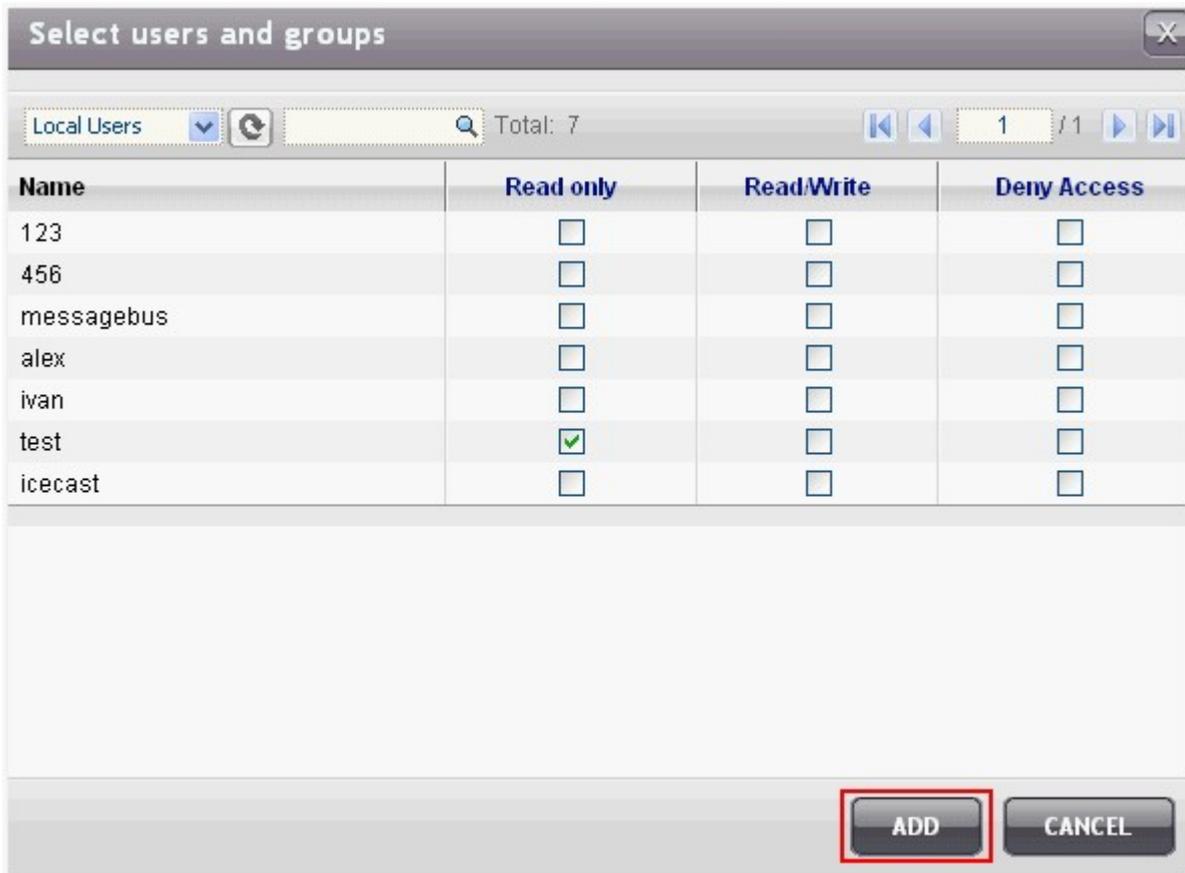
Select the root folder (Dept). Click "+ Add" to specify read only, read/write, or deny access for the users and user groups.



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 .

Share Folders

SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Folder Name:	Permission:	Read only	Read/Write	Deny Access	Special Permission
Dept	everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin	admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HR	test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Production					
Sales					
test					

Guest Access Right:

Owner: admin  Only the owner can delete the contents ([see online help](#))

Only admin can create files and folders ([see online help](#))
 Apply changes to files and sub-folders
 Apply and replace all existing permissions of this folder, files, and subfolders

For detailed instructions, please [click here](#)

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

Local Users

Search to select the user or user group:

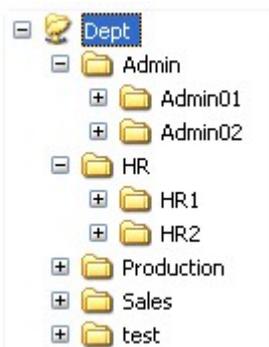
admin
123
456
messagebus
alex
ivan
test
icecast

- 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.

The screenshot shows the 'Share Folders' configuration page. A dialog box is overlaid on the page, asking for confirmation to apply permissions. The 'YES' button in the dialog is highlighted with a red box. In the background, the 'Share Folders' window is visible, showing a folder tree on the left and a table of permissions on the right. The 'APPLY' button at the bottom right of the window is also highlighted with a red box.

Folder Name:	Write	Deny Access	Special Permission
Dept	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HR	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Production	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Guest Access Right: Deny access

Owner: admin

Only the owner can delete the contents (see online help)

Only admin can create files and folders (see online help)

Apply changes to files and sub-folders

Apply and replace all existing permissions of this folder, files, and subfolders

For detailed instructions, please [click here](#)

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.

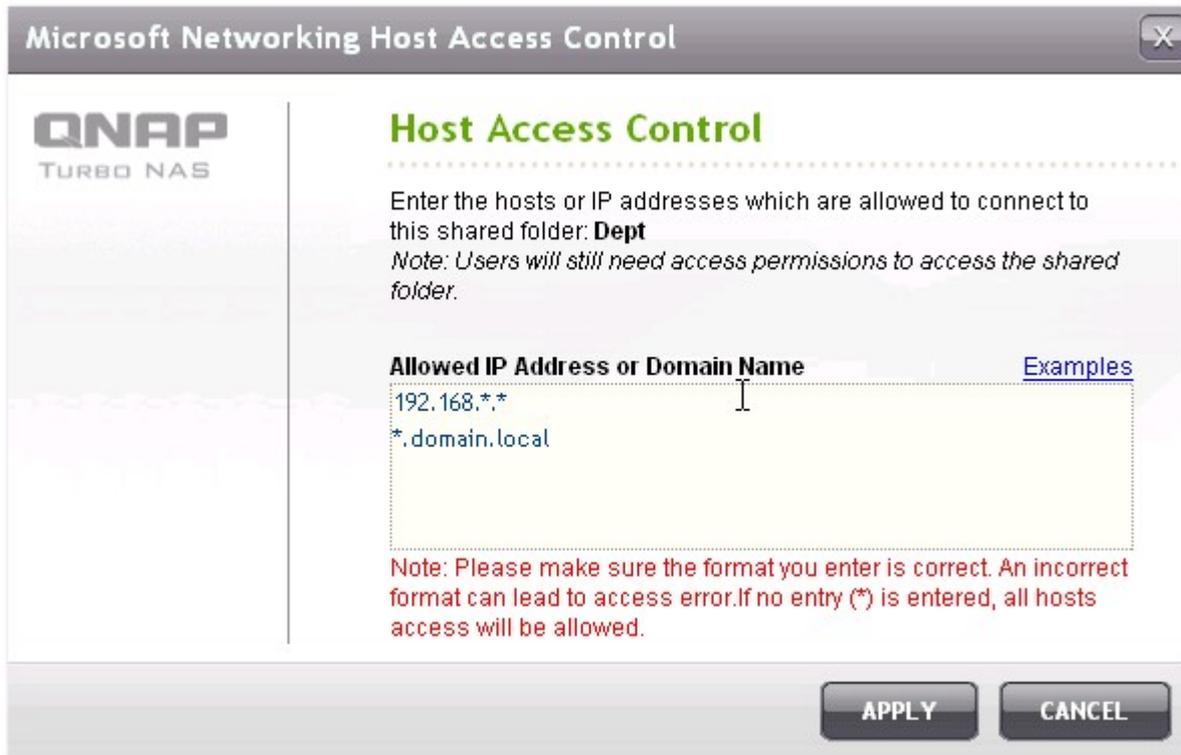


The screenshot shows the 'Share Folders' management interface. At the top, there are tabs for 'SHARE FOLDERS', 'ISO SHARE FOLDERS', 'FOLDER AGGREGATION', and 'ADVANCED OPTIONS'. Below the tabs, there is a search bar for 'Shares' and two buttons: 'New Share Folder' and 'Restore Default Network Shares'. The main area contains a table with the following data:

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Dept	40 KB	9	0	No	NFS
<input type="checkbox"/>	Download	400.2 MB	7	8	No	NFS
<input type="checkbox"/>	Multimedia	12.84 GB	65	575	No	NFS
<input type="checkbox"/>	Network Recycle Bin 1	28 KB	4	2	No	NFS
<input type="checkbox"/>	Public	26.55 GB	319	1650	No	NFS
<input type="checkbox"/>	Recordings	88 KB	19	2	No	NFS

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.

Create An ISO Share Folder [X]

QNAP
TURBO NAS

ISO Share Folder Settings

Folder Name:

Hide Folder: Yes No ⓘ

Description:

Step 2 of 7

BACK **NEXT** **CANCEL**

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".

Create An ISO Share Folder [X]

QNAP
TURBO NAS

Privilege

You can select one of the following methods to configure the user access right to the network share folder:

- Grant read-only access right for administrators only
- By User
- By User Group

Guest Access Right:

- Deny Access
- Read only

Step 3 of 7

BACK **NEXT** **CANCEL**

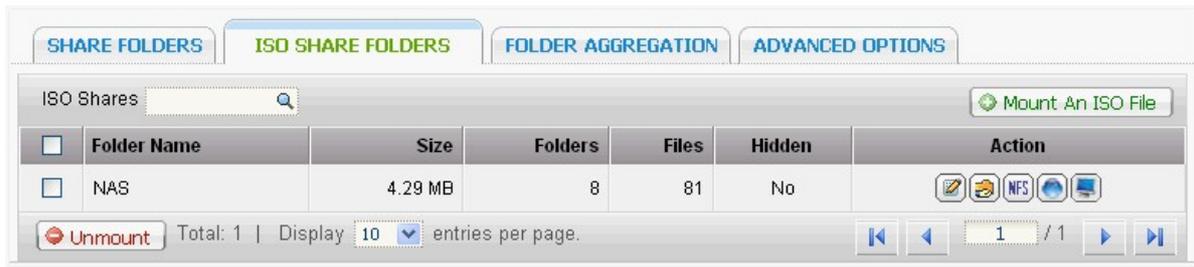
5. Confirm the settings and click "Next".



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 here³¹⁴ 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.

The screenshot shows the 'Share Folders' configuration interface. At the top, there are four tabs: 'SHARE FOLDERS', 'ISO SHARE FOLDERS', 'FOLDER AGGREGATION' (which is selected and highlighted in green), and 'ADVANCED OPTIONS'. Below the tabs, the 'Folder Aggregation' section is visible. It contains a checkbox labeled 'Enable Folder Aggregation' which is checked. Below the checkbox, there is explanatory text: 'Enable this function will allow you to aggregate all shared folders in local network into a "portal folder" in your NAS.' and 'Folder Aggregation is for Microsoft Network / Samba Service ONLY.' At the bottom right of this section is an 'APPLY' button. Below the 'Folder Aggregation' section is the 'Folder Aggregation List' section. It features two buttons: 'Create A Portal Folder' and 'Import/ Export Folder Tree'. Below these buttons is a table with two columns: 'Portal Folder Name' and 'Action'. The 'Action' column contains a 'Delete' button with a red trash icon.

2. Click "Create A Portal Folder".

This is a close-up screenshot of the 'Folder Aggregation List' section from the previous image. It shows the two buttons 'Create A Portal Folder' and 'Import/ Export Folder Tree'. The 'Create A Portal Folder' button is highlighted with a red rectangular box. Below the buttons is the table with columns 'Portal Folder Name' and 'Action', and a 'Delete' button in the 'Action' column.

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

Create A Portal Folder ✕

QNAP
TURBO NAS

Create A Portal Folder

Folder Name: ✓

Hide Folder: Yes No ⓘ

Comment:

Step 1 of 1

APPLY **CANCEL**

- 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.

Folder Aggregation List

<input type="checkbox"/>	Portal Folder Name	Action
<input type="checkbox"/>	Shares	 

Remote Folder Link X

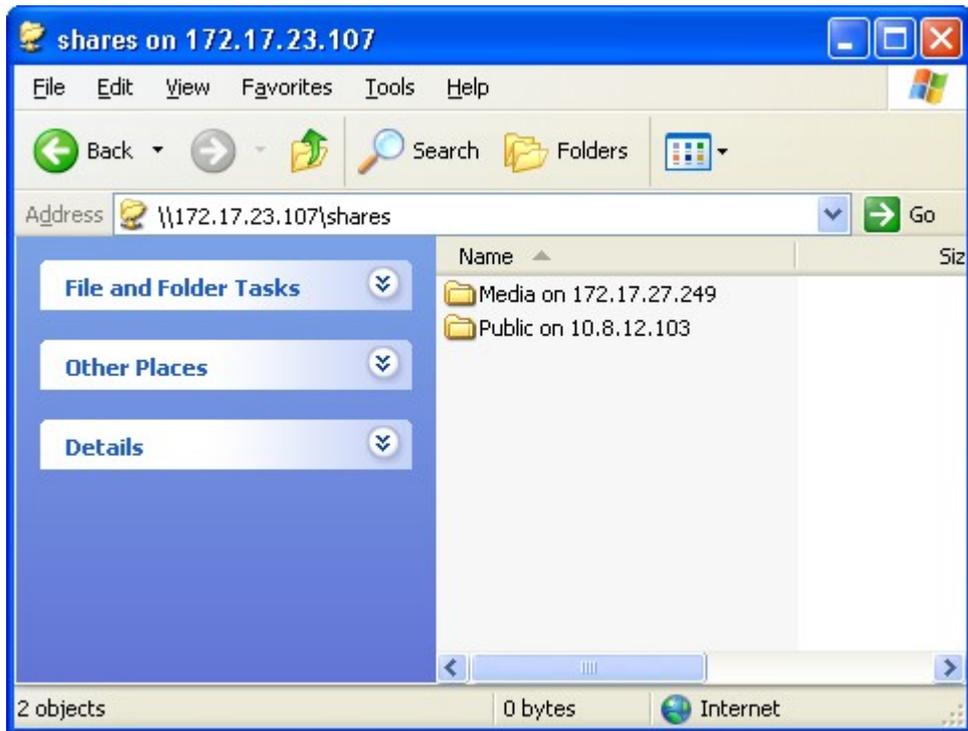
Remote Folder Link

Portal Folder Name: Shares

Link	Name	Host Name	Remote Share Folder
1	Public on 10.8.12.103	10.8.12.103	Public
2	dia on 172.17.27.249	172.17.27.249	Media
3			
4			
5			
6			
7			
8			
9			
10			

Step 1 of 1

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.

Share Folders

SHARE FOLDERS
ISO SHARE FOLDERS
FOLDER AGGREGATION
ADVANCED OPTIONS

Advanced Options

When this option is enabled, you can assign the folder and subfolder permission to individual users and user groups.

Enable Advanced Folder Permissions

Enable Windows ACL Support

APPLY

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" ²³⁰ 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

Quota

Enable quota for all users

Quota size on the disk: MB

Note: Individual user quota size can be changed in [Users · Quota Settings \[Users \]](#)

[APPLY](#)

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.

Users	Quota Size	Used Size	Status
admin	--	167 MB	No size limitation
test	1.95 GB	0 MB	Available 1.95 GB
user01	1.95 GB	0 MB	Available 1.95 GB
user02	1.95 GB	0 MB	Available 1.95 GB
user03	1.95 GB	0 MB	Available 1.95 GB
user04	1.95 GB	0 MB	Available 1.95 GB
user05	1.95 GB	0 MB	Available 1.95 GB
guest	1.95 GB	0 MB	Available 1.95 GB

Total: 8 | Display entries per page. 1 / 1

[GENERATE](#) [DOWNLOAD](#)

Note: 2010_05_12_Local_User_Quota_Volume1.csv is ready to be downloaded.

6. Network Services

Microsoft Networking [269](#)

Apple Networking [273](#)

NFS Service [270](#)

FTP Service [279](#)

Telnet/SSH [281](#)

SNMP Settings [282](#)

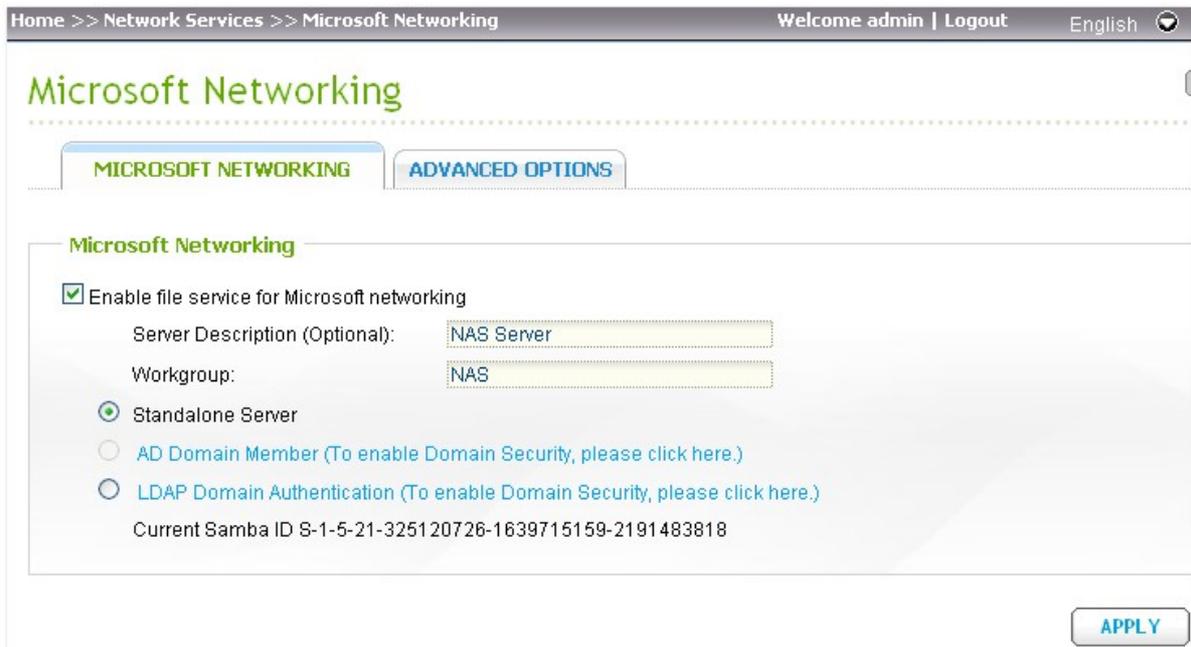
Web Server [284](#)

Network Service Discovery [311](#)

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.



The screenshot shows a web interface for configuring Microsoft Networking. The breadcrumb navigation is "Home >> Network Services >> Microsoft Networking". The user is logged in as "admin" and the language is set to "English". The page title is "Microsoft Networking". There are two tabs: "MICROSOFT NETWORKING" (selected) and "ADVANCED OPTIONS". The main content area is titled "Microsoft Networking" and contains the following settings:

- Enable file service for Microsoft networking
 - Server Description (Optional):
 - Workgroup:
- Standalone Server
- AD Domain Member (To enable Domain Security, please click here.)
- LDAP Domain Authentication (To enable Domain Security, please click here.)

Current Samba ID S-1-5-21-325120726-1639715159-2191483818

An "APPLY" button is located at the bottom right of the configuration area.

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

The screenshot shows the 'Microsoft Networking' configuration window with the 'ADVANCED OPTIONS' tab selected. The 'Advanced Options' section contains the following settings:

- Enable WINS server
- Use the specified WINS server
WINS server IP address: [0] [0] [0] [0]
- Local Master Browser
- Allow only NTLMv2 authentication.
- Name Resolve Priority: DNS only (dropdown menu)
- Login style: DOMAIN\USERNAME instead of DOMAIN+USERNAME for FTP, AFP, & Web File Manager
- Automatically register in DNS
- Enable trusted domains

An 'APPLY' button is located in the bottom right corner of the window.

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.

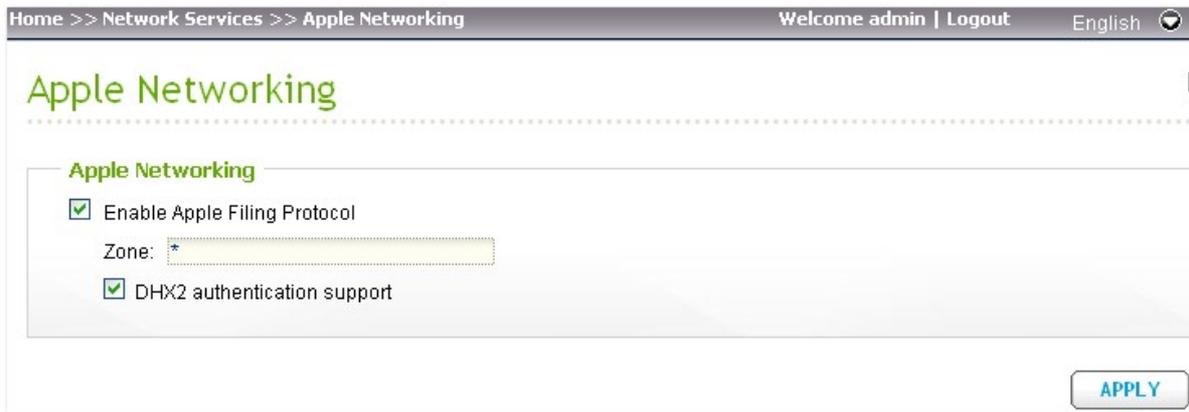
Automatically register in DNS: When this option is turned on and the NAS is joined to an Active Directory, the NAS will register itself automatically in the domain DNS server. This will create a DNS host entry for the NAS in the DNS server. If the NAS IP is changed, the NAS will automatically update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

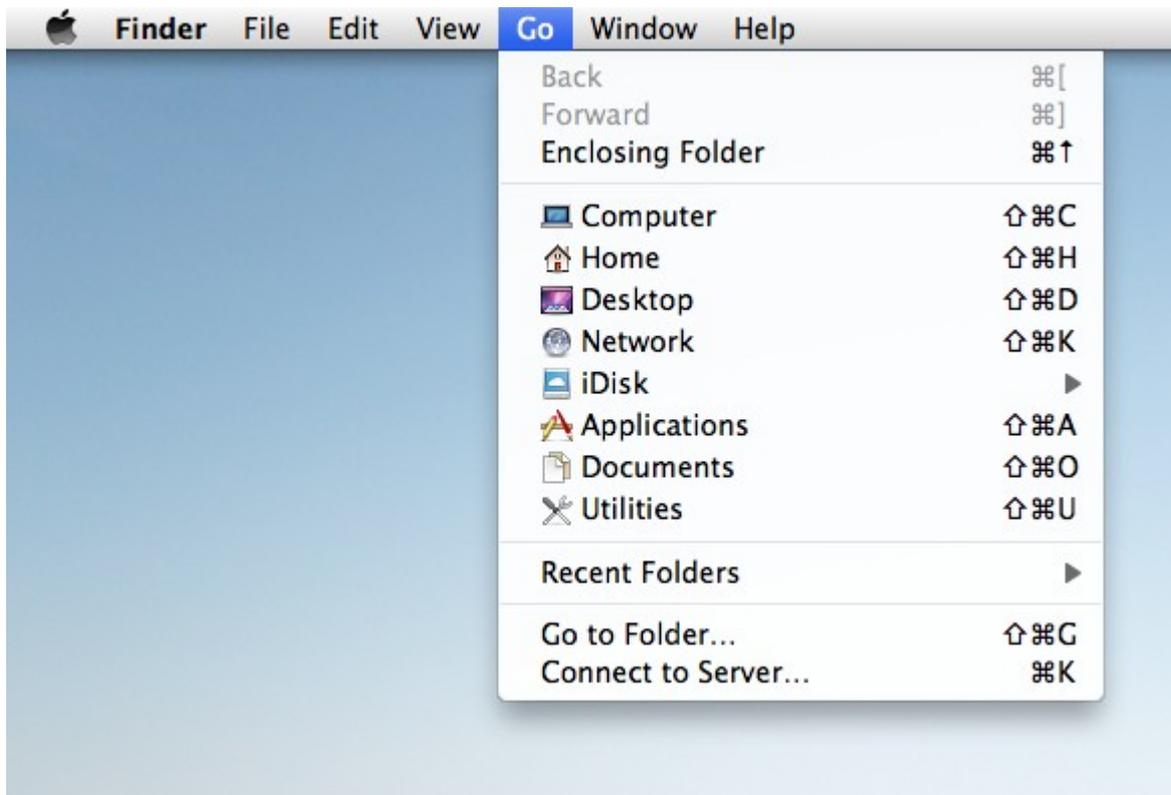
To connect to the NAS from Mac, enable Apple Filing Protocol. If the AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the NAS. Enter an asterisk (*) to use the default setting. This setting is disabled by default.

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



The screenshot shows a web interface for configuring Apple Networking. The breadcrumb trail at the top reads "Home >> Network Services >> Apple Networking". The user is logged in as "admin" and the language is set to "English". The main heading is "Apple Networking". Underneath, there is a section titled "Apple Networking" containing three settings: "Enable Apple Filing Protocol" (checked), "Zone:" (with a text input field containing an asterisk "*"), and "DHX2 authentication support" (checked). An "APPLY" button is located at the bottom right of the configuration area.

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".

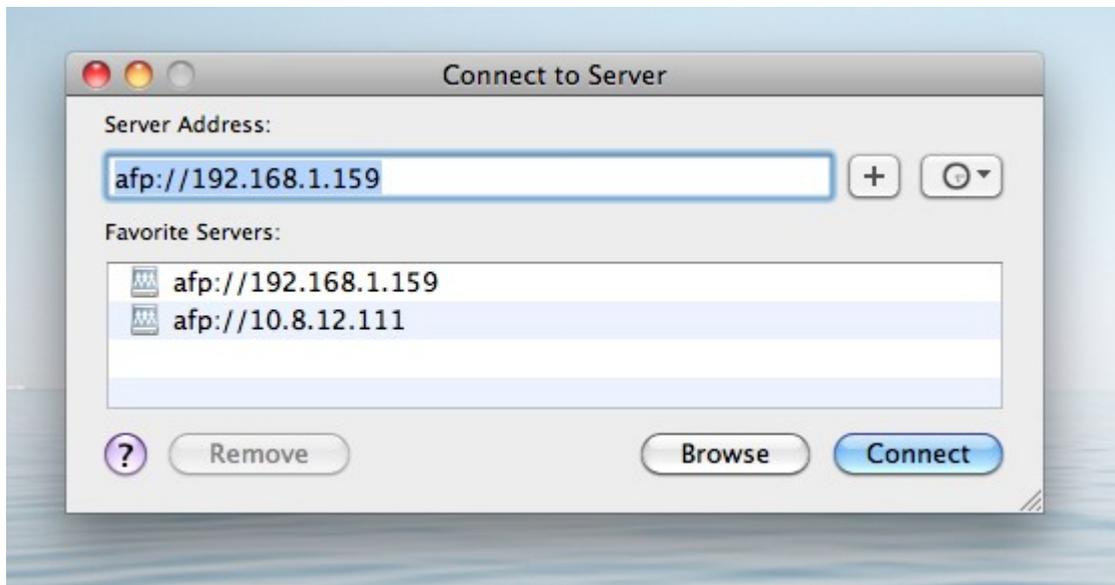


Enter the connection information in the "Server Address" field, such as "afp://YOUR_NAS_IP_OR_HOSTNAME". Here are some examples:

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.

NFS Service

NFS Service

Enable NFS Service

You can set the allowed domain name and the access authority in Share Folder Management.
[Click here to set the NFS access right of the network share.](#)

APPLY

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.

Home >> Access Right Management >> Share Folders Welcome admin | Logout English

Share Folders

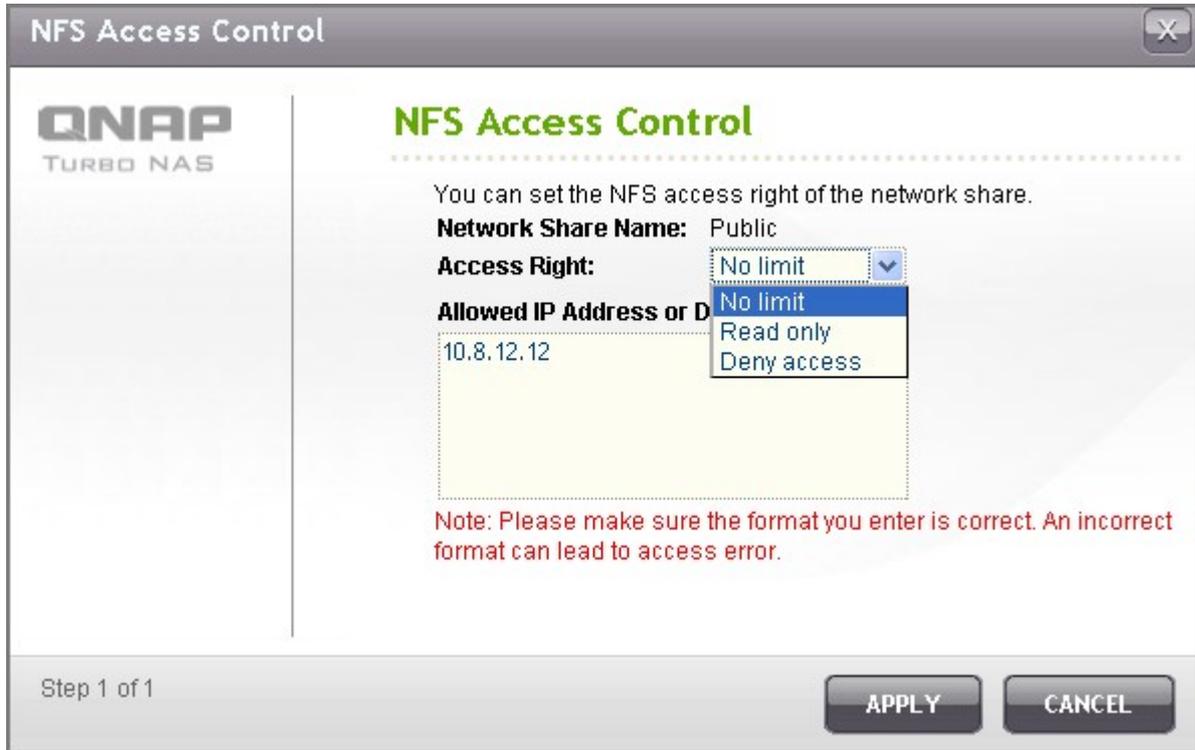
SHARE FOLDERS | ISO SHARE FOLDERS | FOLDER AGGREGATION | ADVANCED OPTIONS

Shares New Share Folder Restore Default Network Shares

<input type="checkbox"/>	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Dept	80 KB	17	2	No	  NFS   
<input type="checkbox"/>	Download	400.2 MB	7	8	No	  NFS   
<input type="checkbox"/>	Multimedia	12.84 GB	65	575	No	  NFS   
<input type="checkbox"/>	Network Recycle Bin 1	120.13 MB	22	27	No	  NFS   
<input type="checkbox"/>	Public	26.55 GB	319	1650	No	  NFS   

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.

FTP Service

General

Enable FTP Service

Protocol Type: FTP (standard) FTP with SSL/TLS (Explicit)

Port Number:

Unicode Support: Yes No

Enable Anonymous: Yes No

Note: If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from [\[Filename Encoding\]](#) under [General Settings] so that the folders and files on FTP can be properly shown.

Connection

Maximum Number of all FTP connections:

Maximum Number of Connections For a Single Account:

Enable FTP transfer limitation

Maximum upload rate (KB/s): KB/s

Maximum download rate (KB/s): KB/s

Advanced

Passive FTP Port Range: Use the default port range (55536 - 56559) Define port range: -

Respond with external IP address for passive FTP connection request

External IP address:

To use the FTP service of the NAS, enable this function. Open an IE browser and enter ftp://NAS IP. Enter the username 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 username 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.

Telnet / SSH

Telnet / SSH

After enabling this option, you can access this server via Telnet or SSH connection. (Only the account admin can login remotely.)

Allow Telnet connection
Port Number:

Allow SSH connection
Port Number:

Enable SFTP

[APPLY](#)

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:

SNMP Trap Level: Information Warning Error

Trap Address 1:

Trap Address 2:

Trap Address 3:

SNMP Version:

Community:

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.

Home >> Network Services >> Web Server Welcome admin | Logout English

Web Server

WEB SERVER | VIRTUAL HOST

Web Server

After enabling this function, you can upload the webpage files to "Web" network share to publish your website.

- Enable Web Server ⓘ
 - Port Number:
 - register_globals: On Off
- Enable Secure Connection (SSL)
 - Port Number:
- Enable WebDAV
- Show service link on the login page

After enabling this service, click the following link to enter to Web Server.

<http://10.8.12.111:80/>
<https://10.8.12.111:8081/>

APPLY

php.ini Maintenance

- php.ini Maintenance

The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.

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.

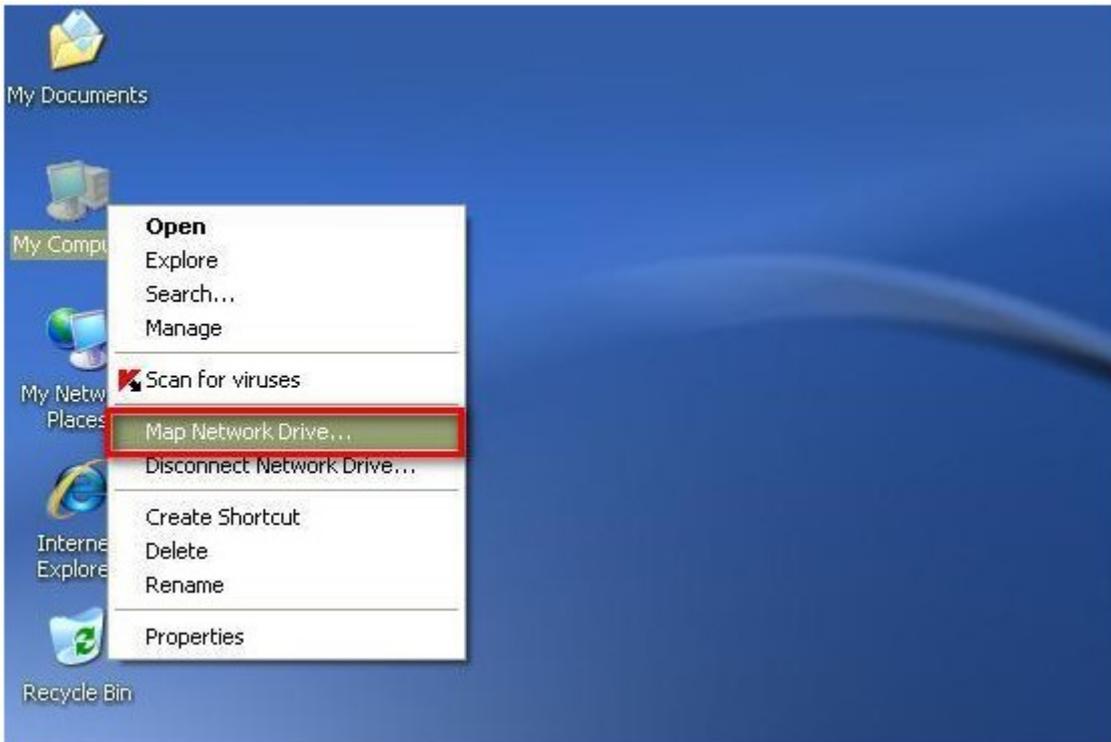
Go to "Access Right Management" > "Share Folders" > "Share Folder". Click the "WebDAV Access Control" button  in the "Action" column, and set the WebDAV access right of the users to the network shares.



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

Windows XP:

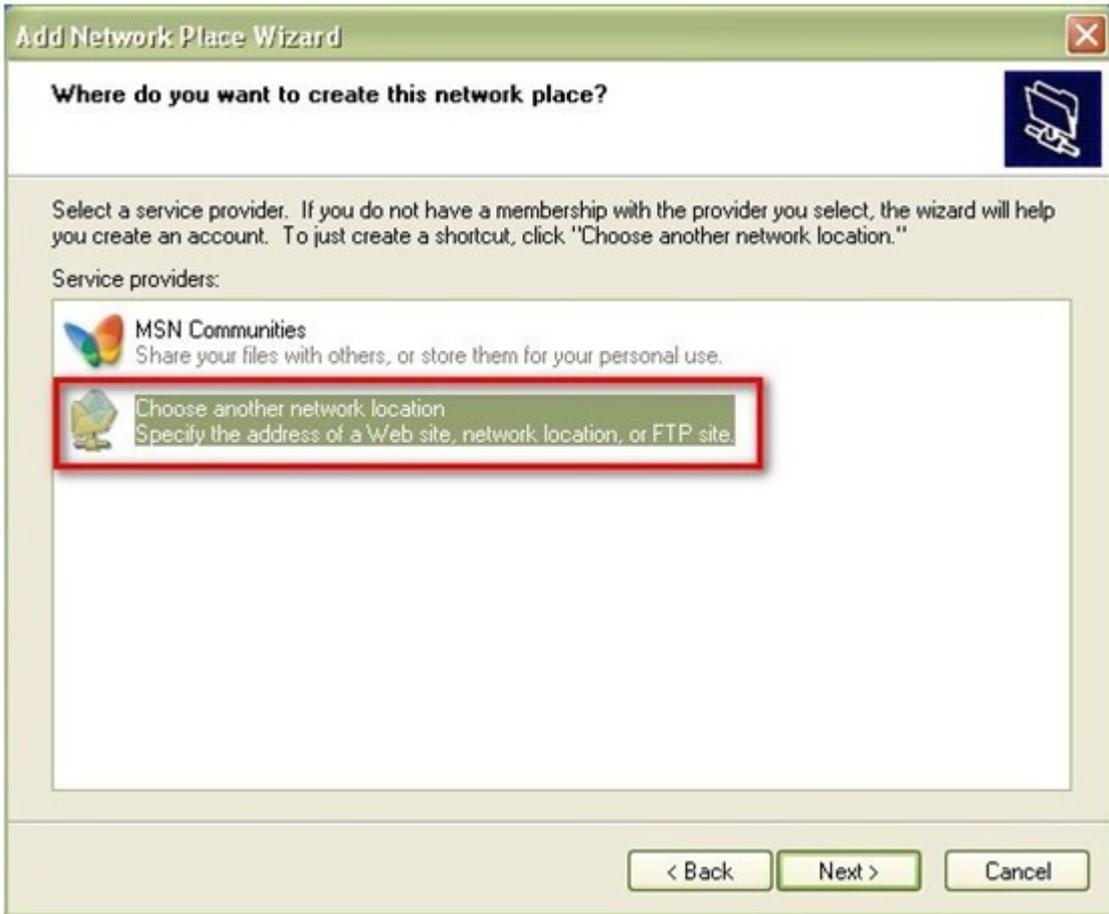
1. Right click "My Computer" and select "Map Network Drive..."



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

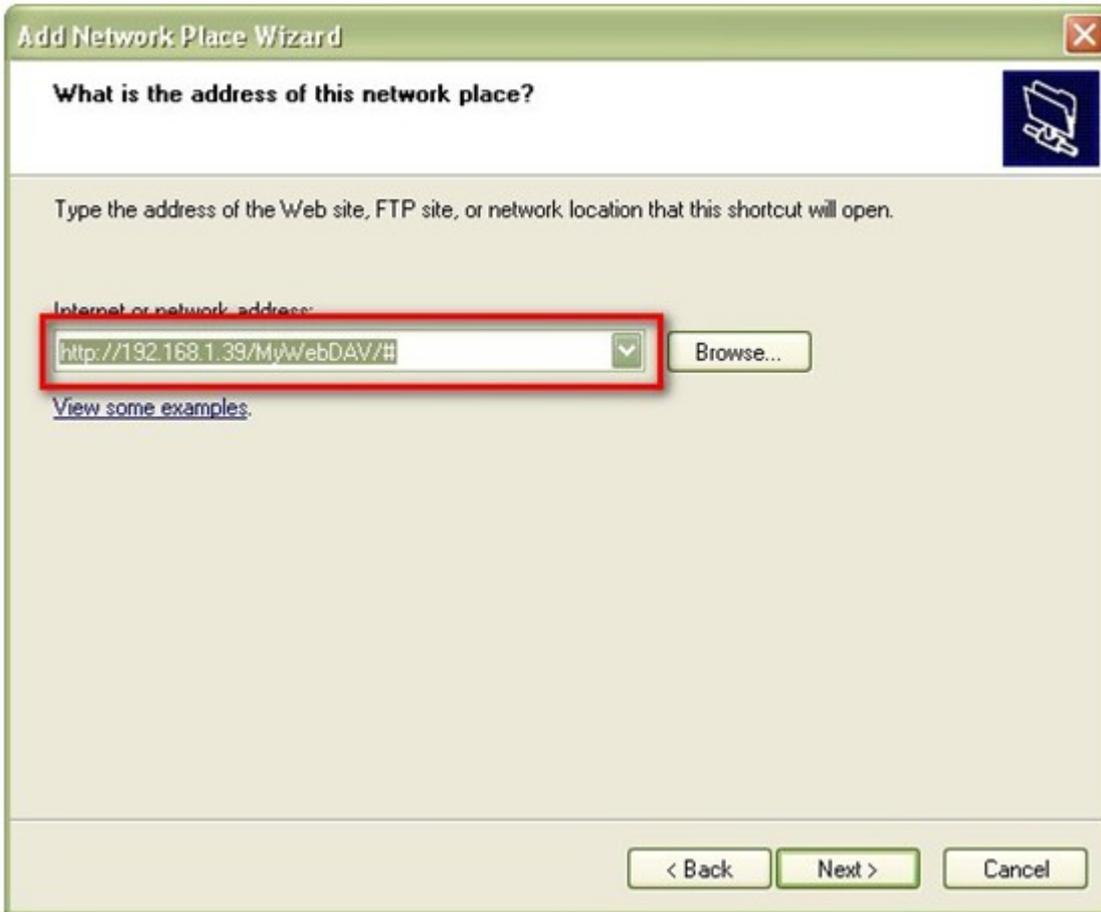


3. Select "Choose another network location".



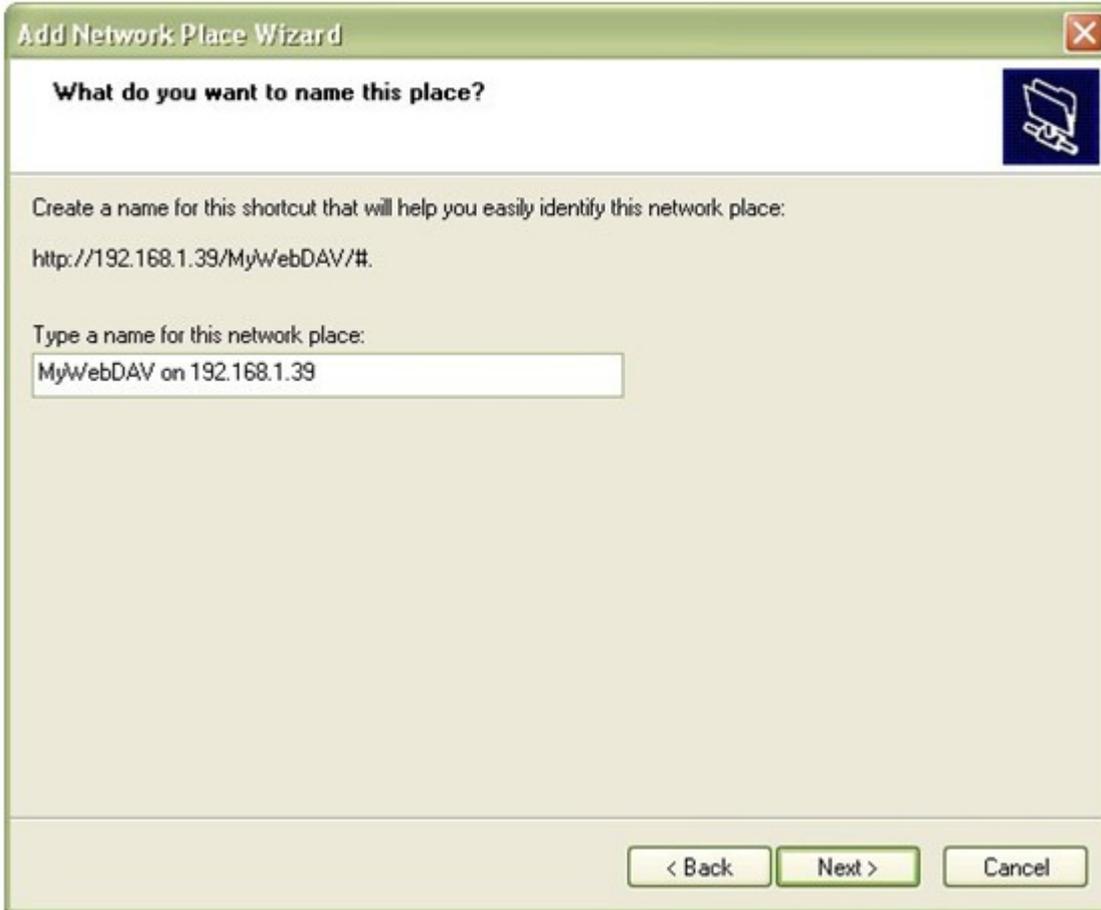
4. Enter the URL of your NAS with the folder name. Note that you should put a “#” key at the end of the URL. Click “Next”.

Format: `http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME/#`

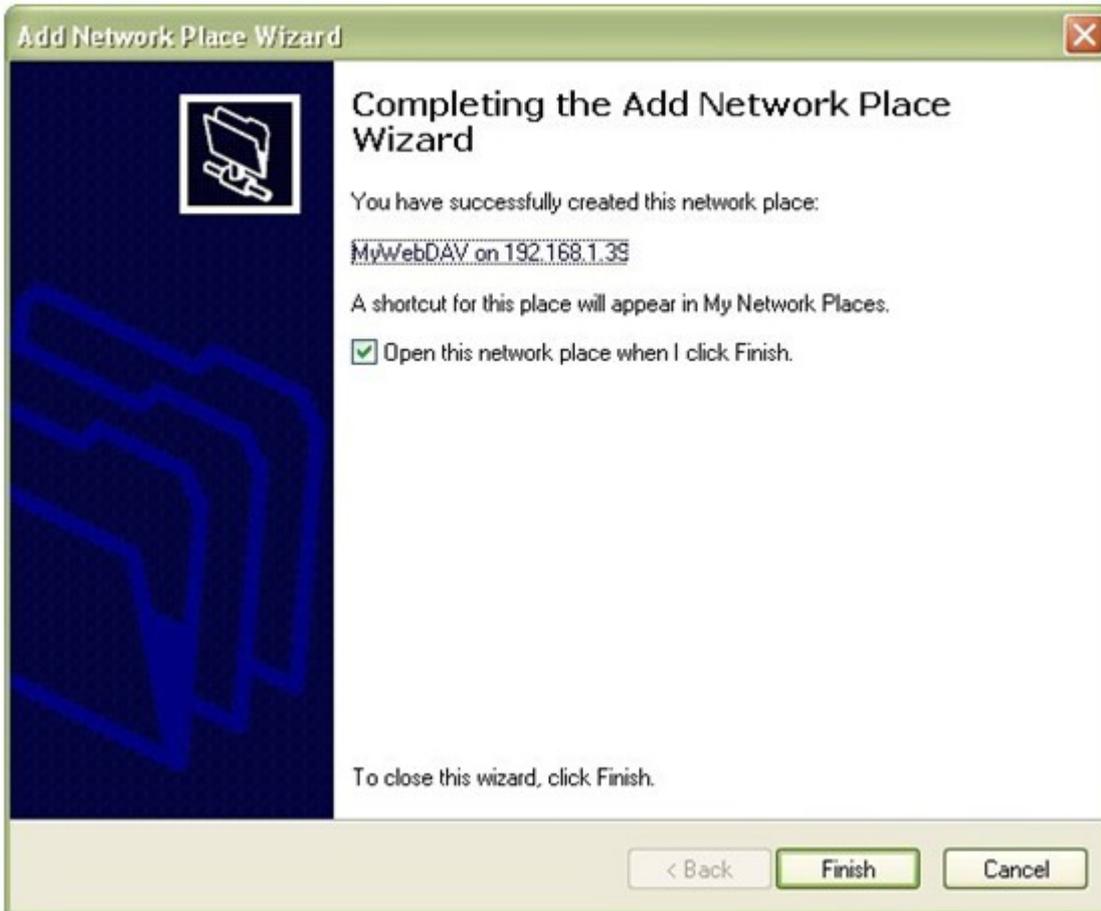


5. Enter the username and password which has the WebDAV access right to connect to the folder.

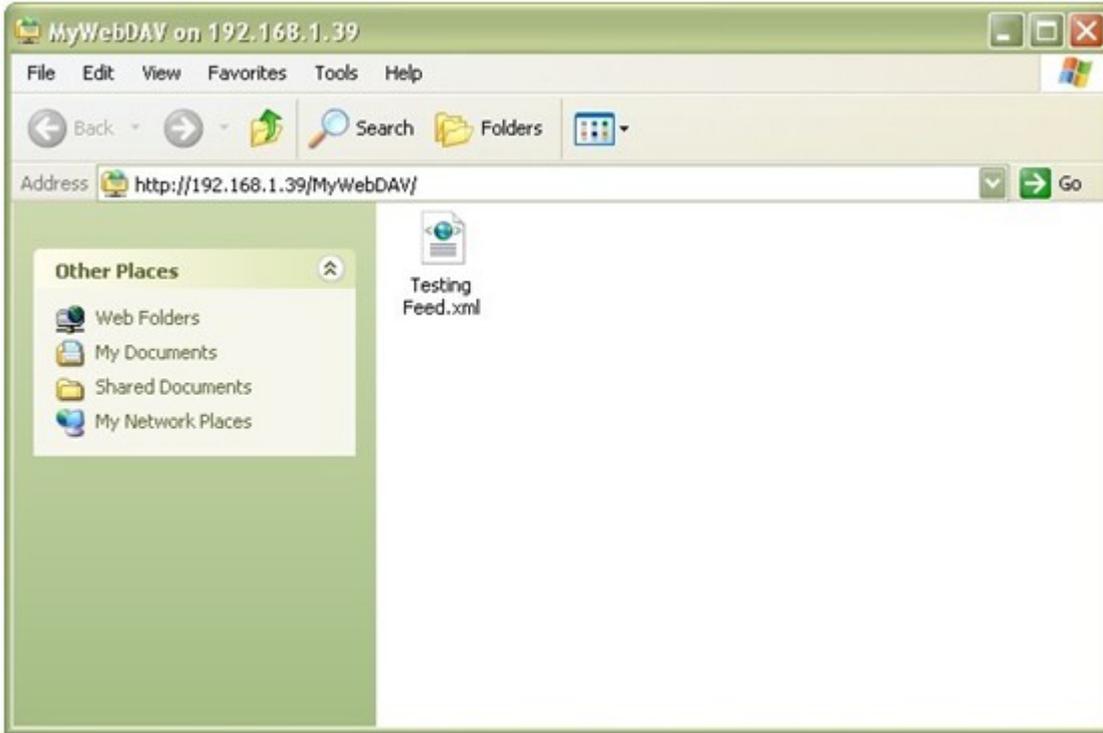
6. Type a name for this network place.



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



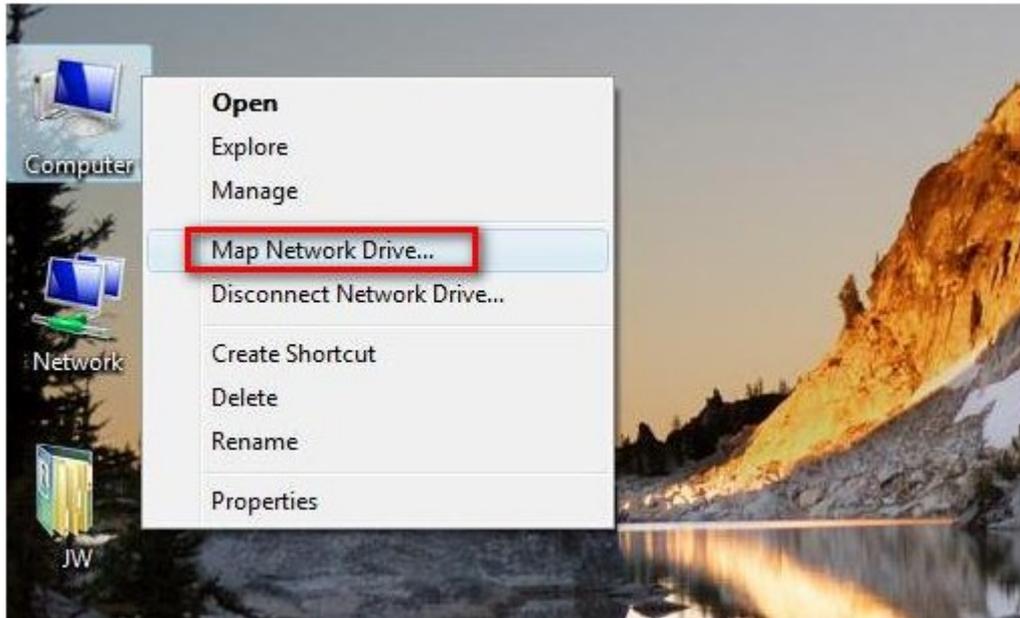
8. Now you can connect to this folder anytime through WebDAV. A shortcut has also been created in "My Network Places".



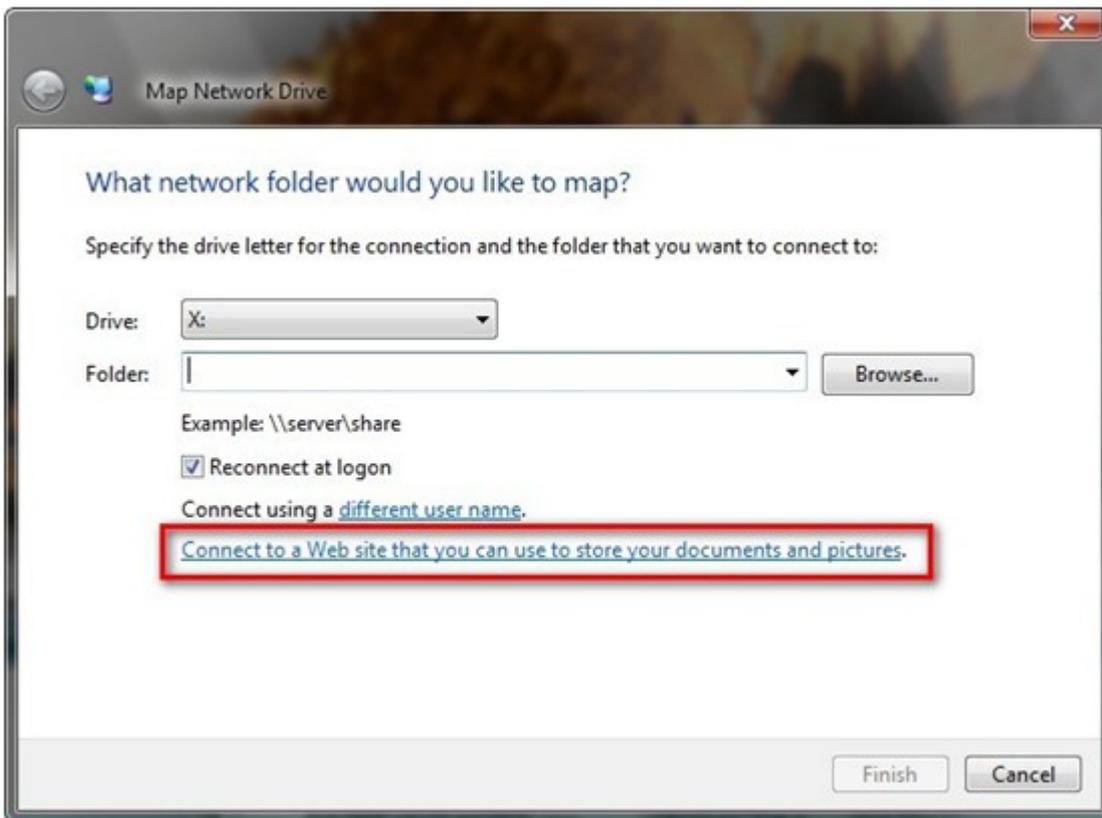
Windows Vista

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>

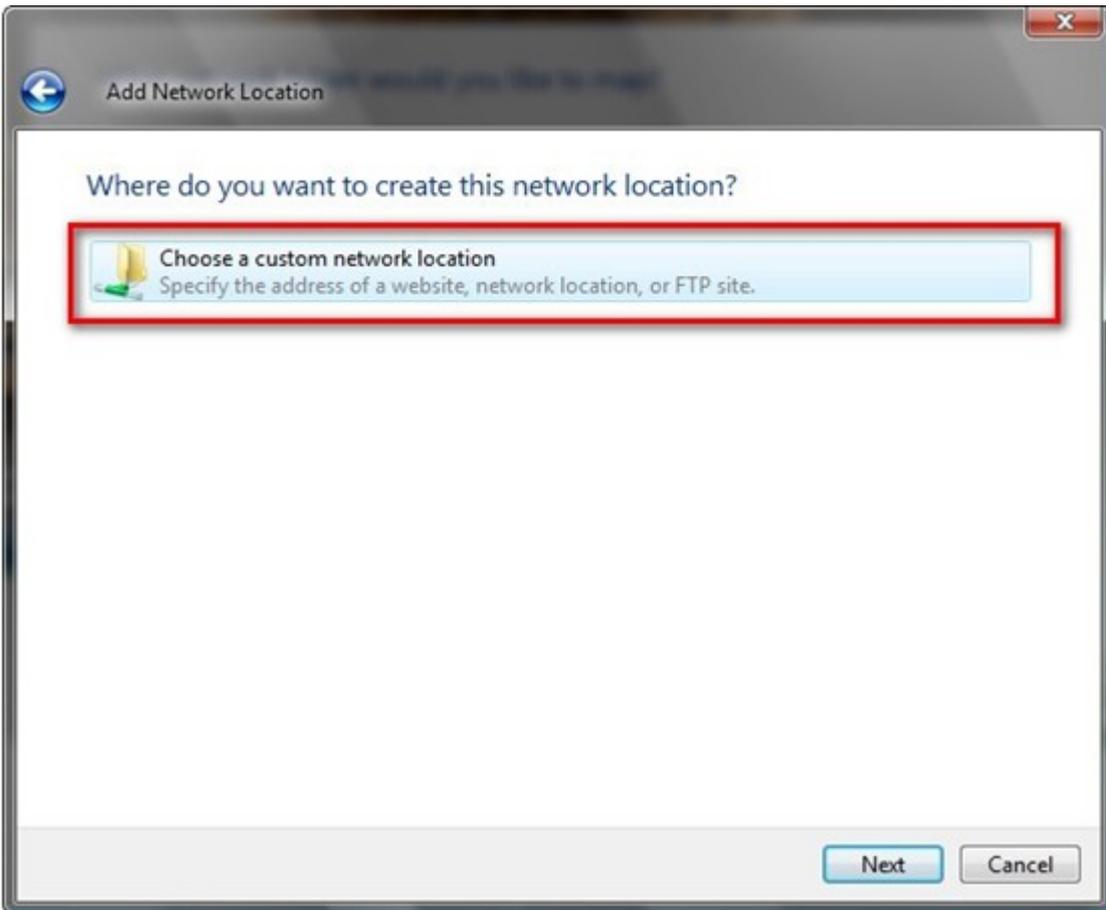
1. Right click "Computer" and select "Map Network Drive..."



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

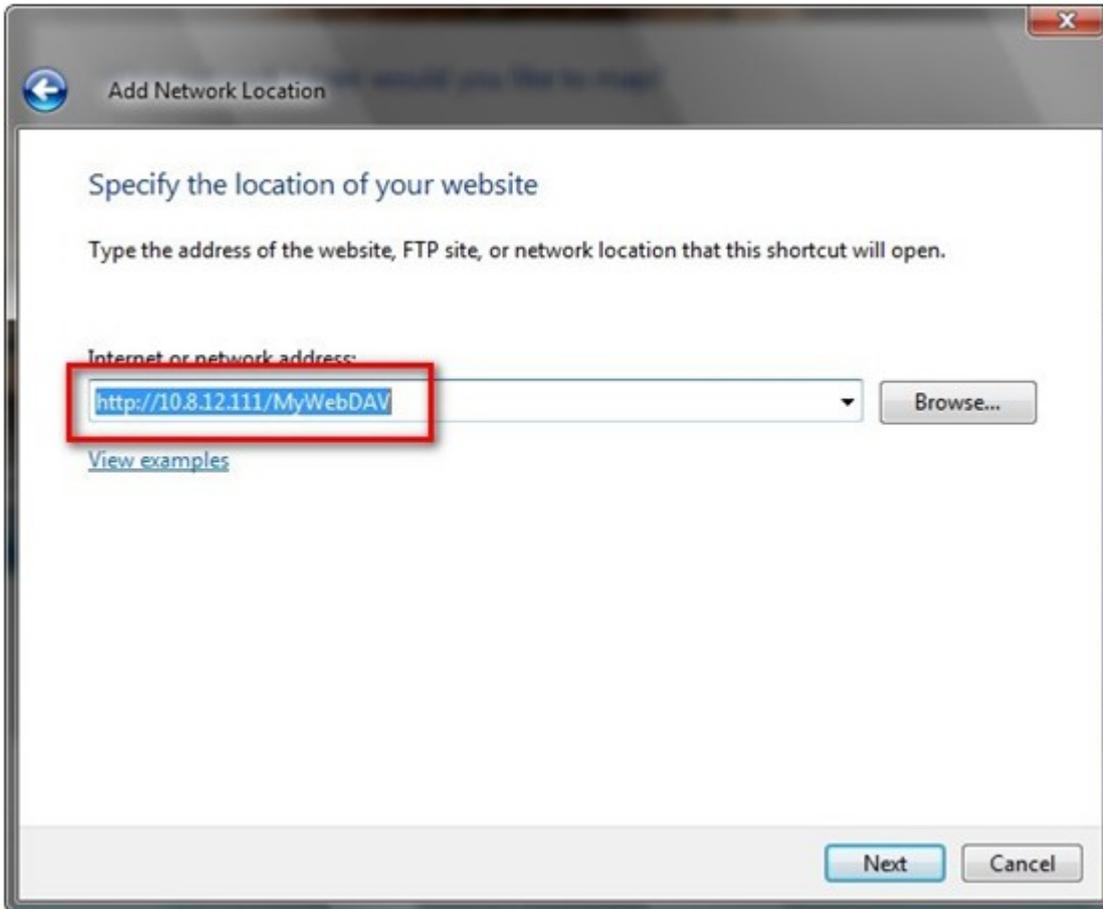


3. Select "Choose a custom network location".



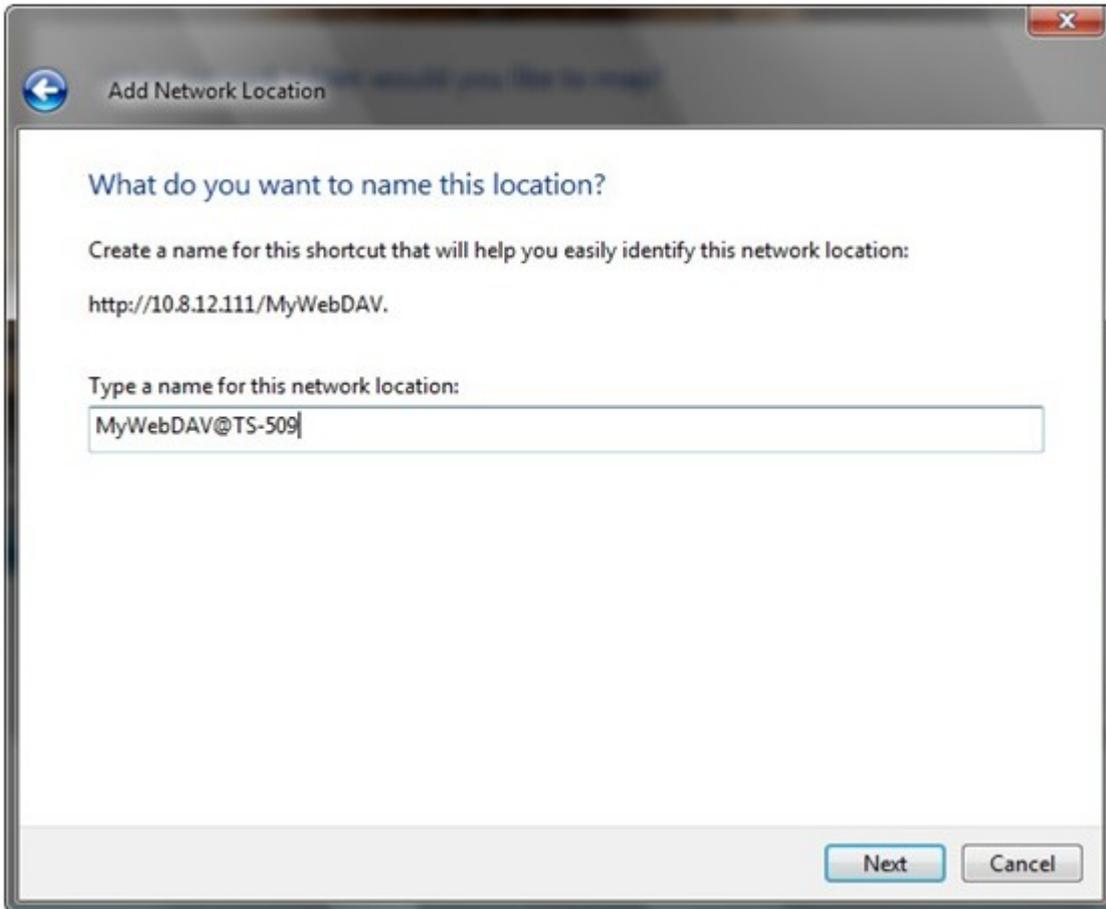
4. Enter the URL of your NAS with the folder name.

Format: `http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME`

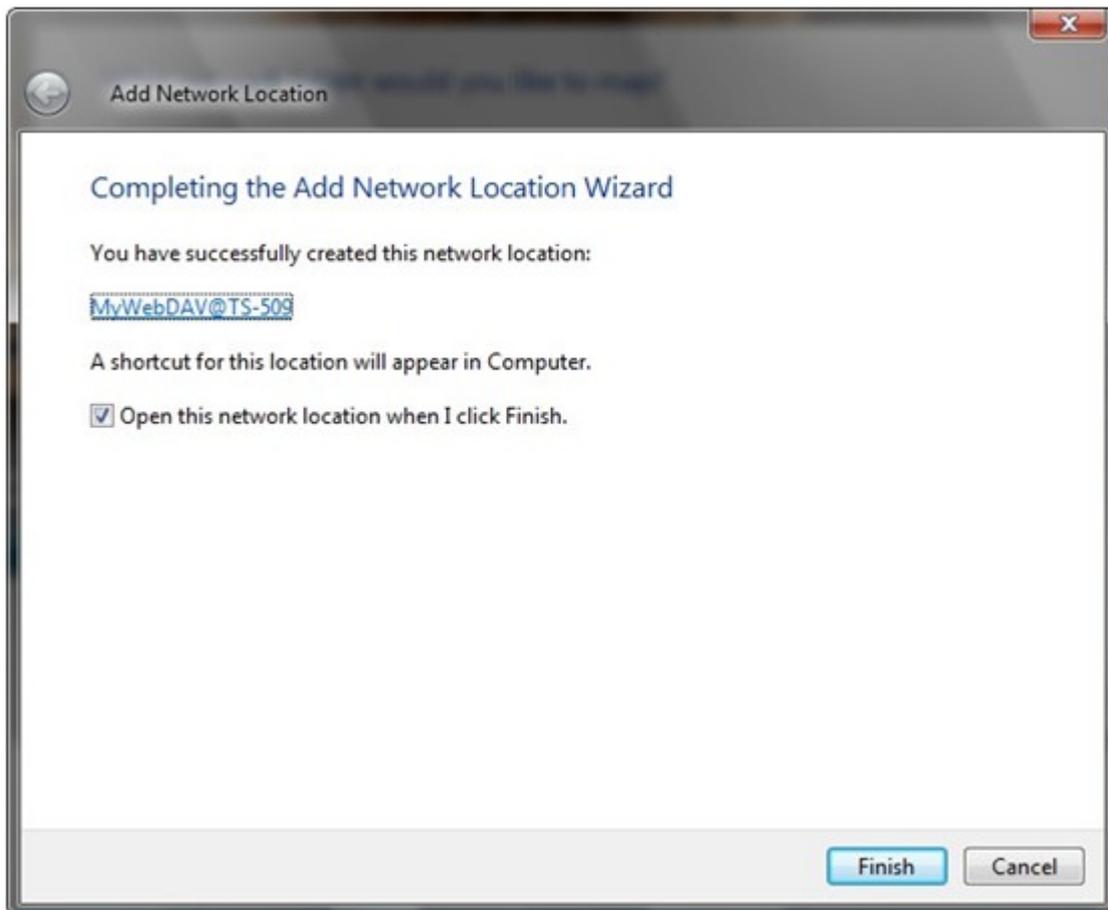


5. Enter the username and password which has the WebDAV access right to connect to this folder.

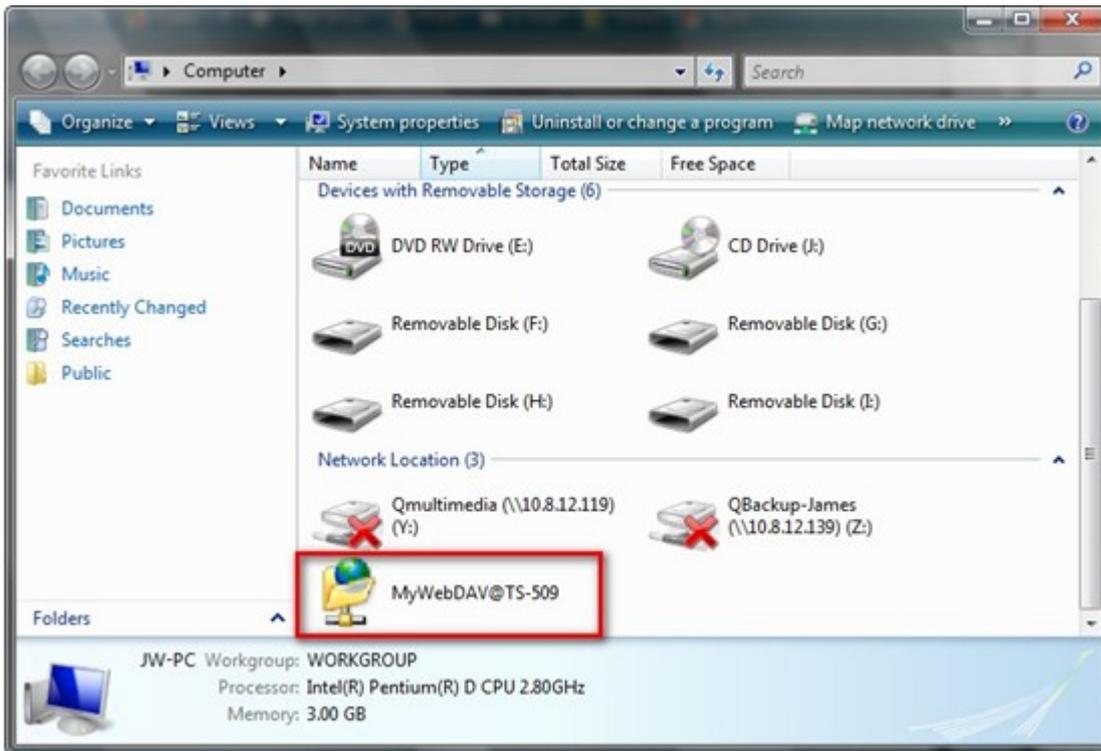
6. Type a name for this network location.



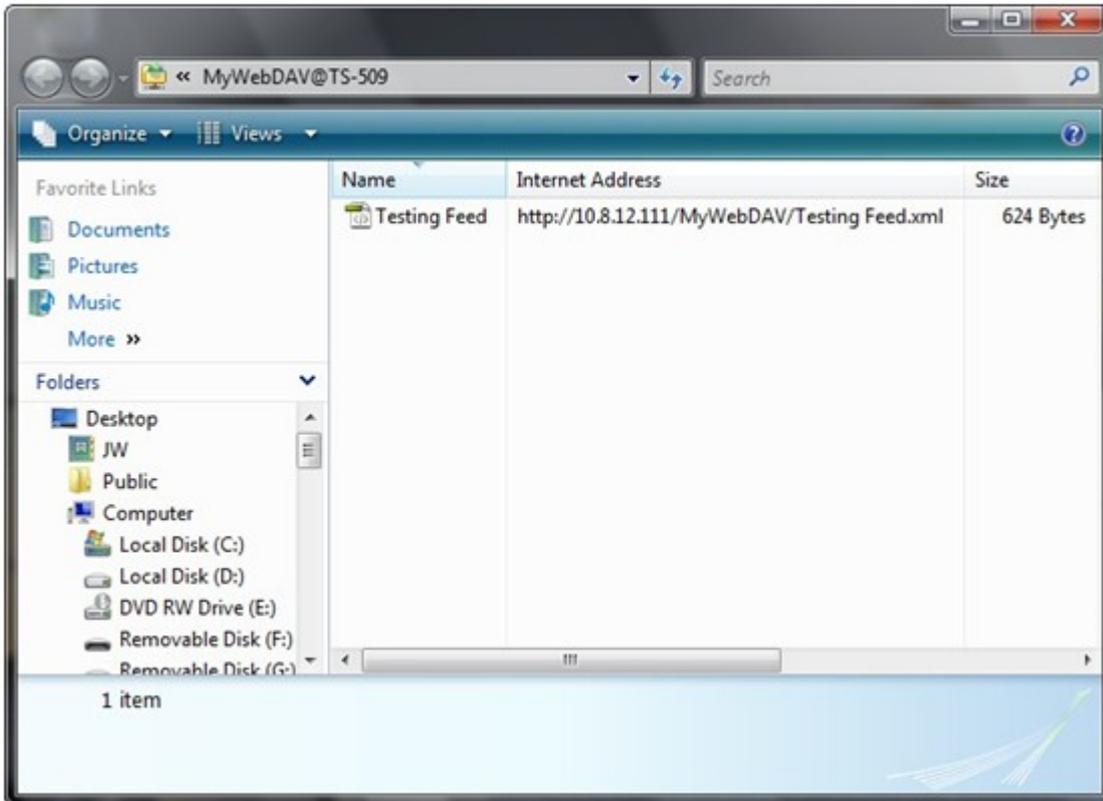
7. The Web folder has been successfully created.



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



9. You can connect to the folder through 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 username 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

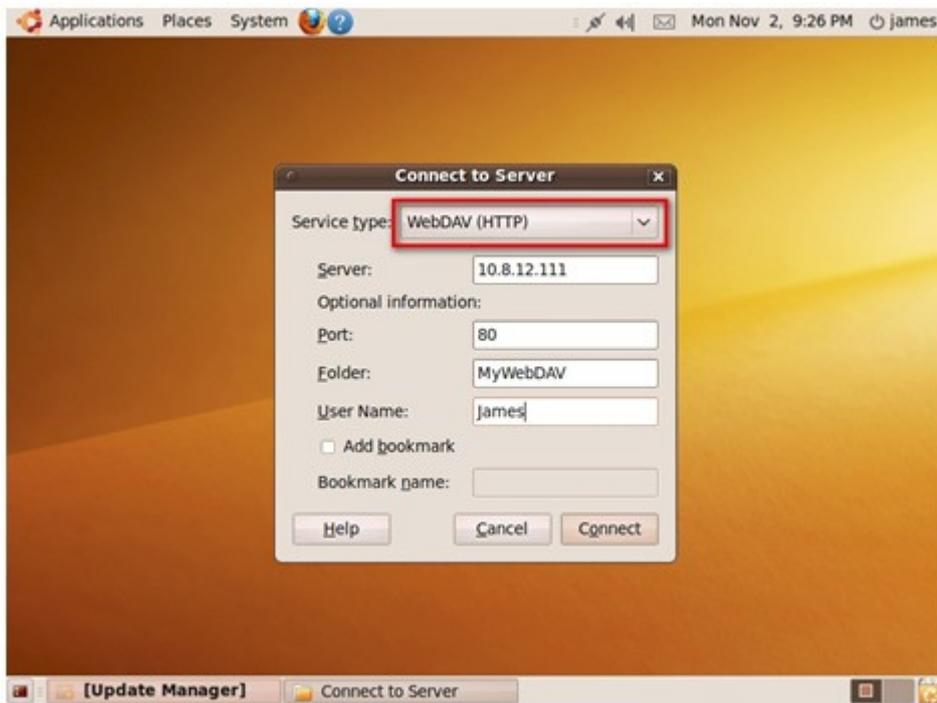
Follow the steps below to connect to your NAS via WebDAV on Ubuntu.

Client Operating System: Ubuntu 9.10 Desktop

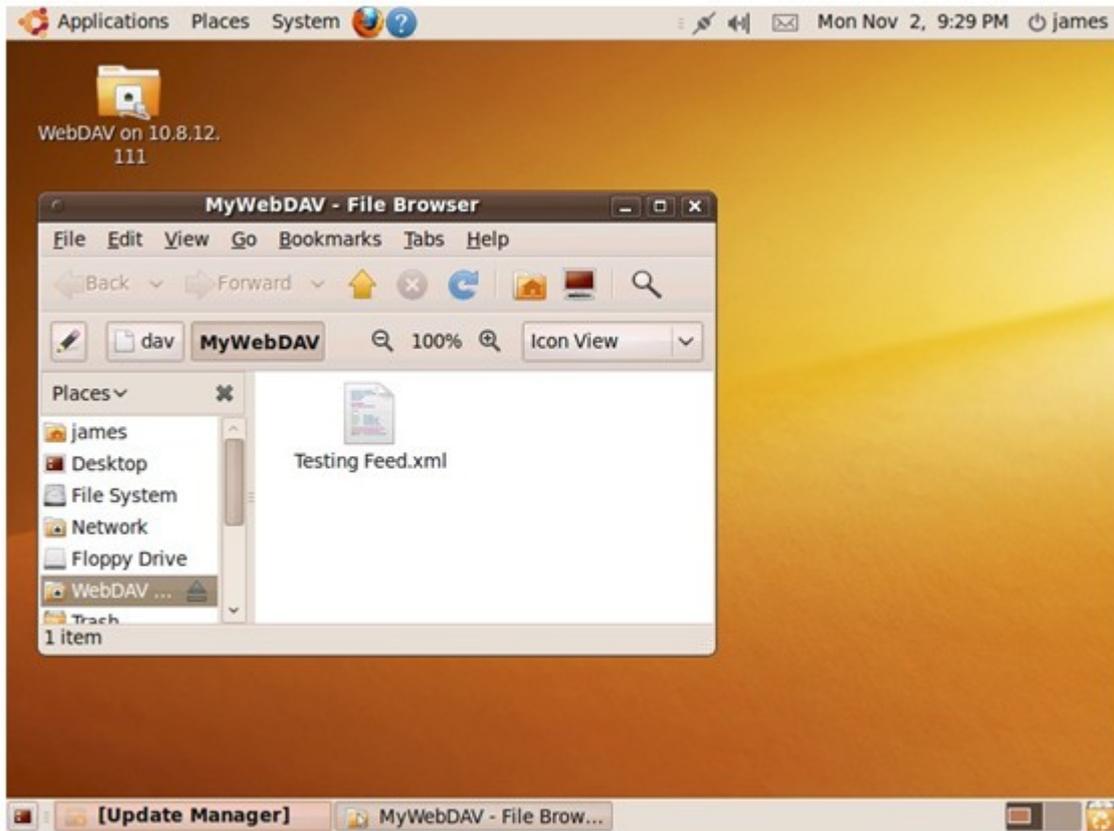
1. Open "Places" > "Connect to Server..."



2. Select "WebDAV (HTTP)" or "Secure WebDAV (HTTPS)" for the Service type according to your NAS settings and enter your host information. Enter the username 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 username 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)	/Qweb/site1_mysite	Joomla!
site2.mysite.com	Port: 80 (NAS)	/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.

Modify Virtual Host
✕



Modify Virtual Host

Host Name:

Folder Name:

Protocol : HTTP HTTPS

Port:

Step 1 of 1

APPLY
CANCEL

Web Server

WEB SERVER

VIRTUAL HOST

Virtual Host

After enabling this function, you can create multiple websites by uploading Web files to each folder.

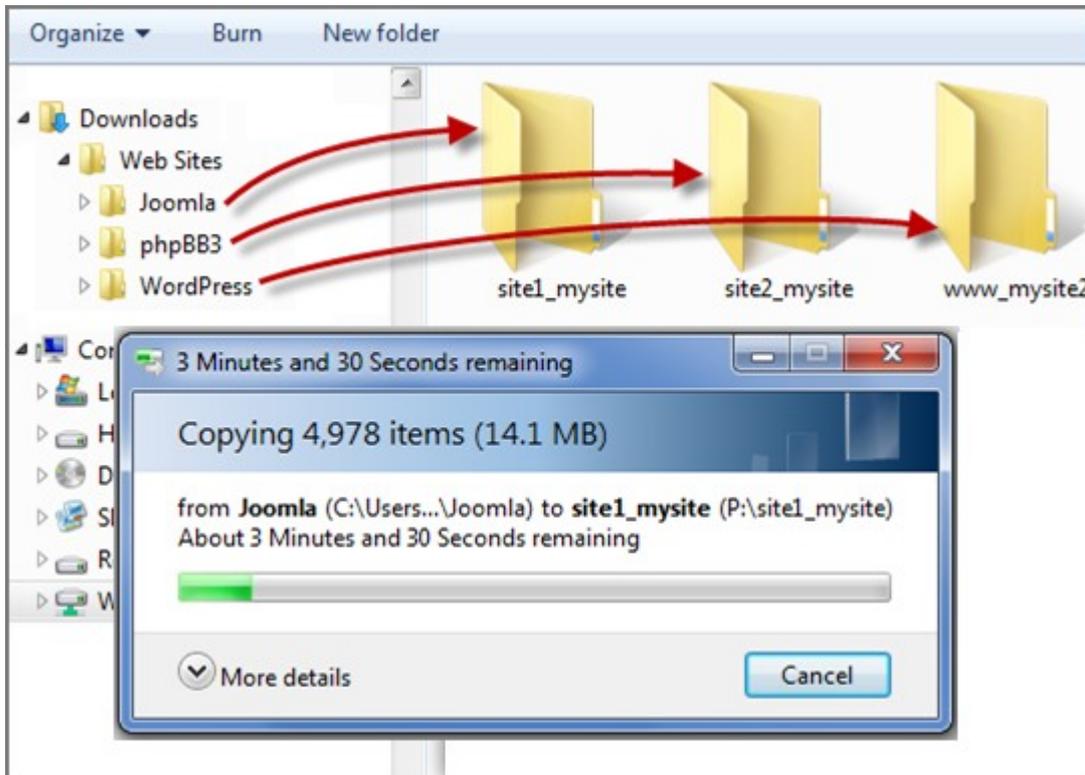
Enable Virtual Host APPLY

Create New Virtual Host

<input type="checkbox"/>	Host Name	Folder Name	Protocol	Port	Action
<input type="checkbox"/>	site1.mysite.com	/Qweb/site1_mysite	HTTP	80	
<input type="checkbox"/>	site2_mysite.com	/Qweb/site2_mysite	HTTP	80	
<input type="checkbox"/>	www.mysite2.com	/Qweb/www_mysite2	HTTP	80	

Delete

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.

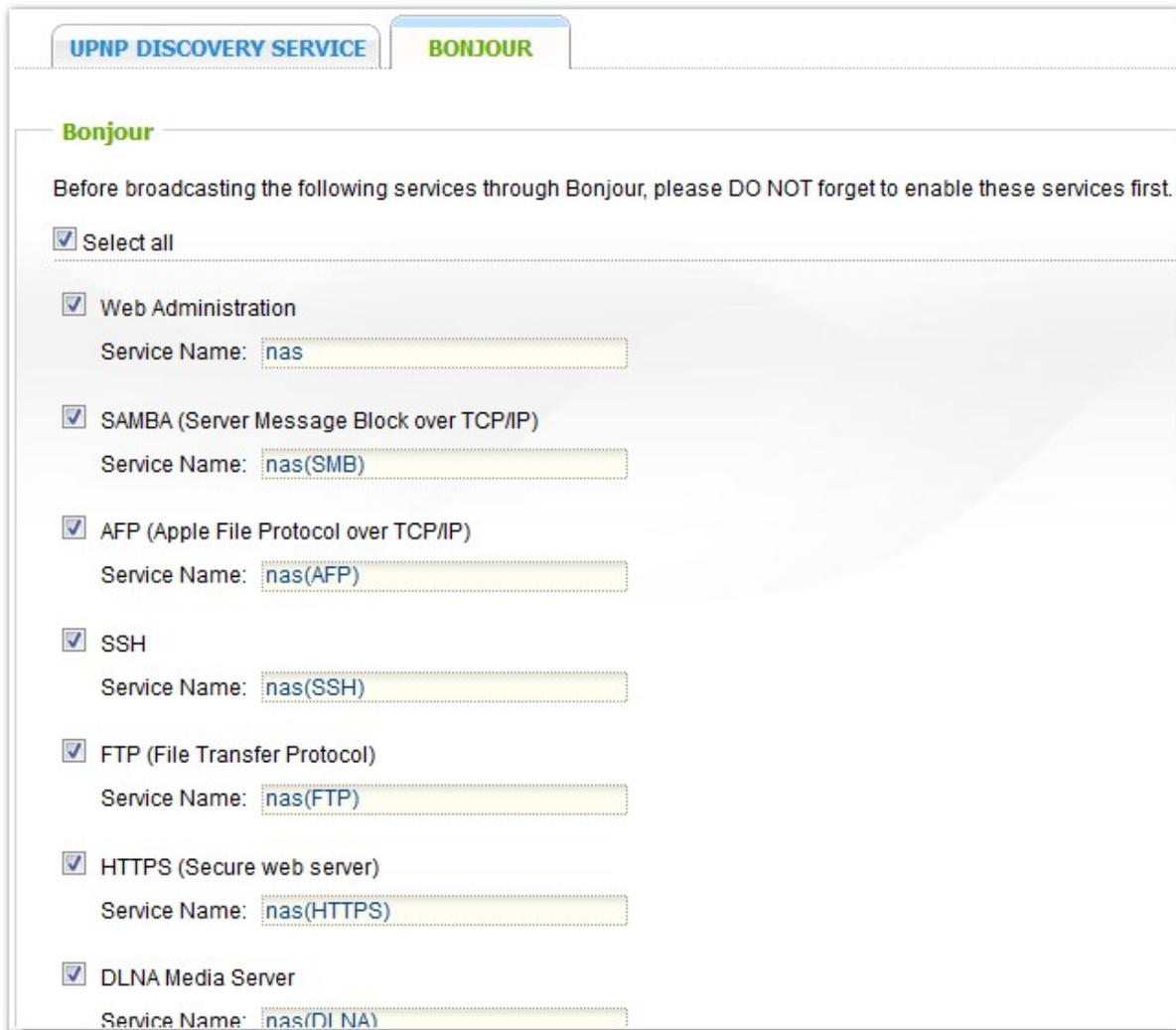
By enabling UPnP Discovery Service, the NAS can be discovered by any operating systems that support UPnP.

The screenshot shows a web interface for configuring Network Service Discovery. At the top, there is a breadcrumb trail: "Home >> Network Services >> Network Service Discovery". On the right side of the header, it says "Welcome admin | Logout" and "English". The main heading is "Network Service Discovery" in green. Below the heading, there are two tabs: "UPNP DISCOVERY SERVICE" (which is selected) and "BONJOUR". Under the "UPNP DISCOVERY SERVICE" tab, there is a section titled "UPnP Discovery Service". Below this title, there is a descriptive text: "After enabling this service, your NAS can be discovered by any operating systems that support UPnP." Below the text, there is a checkbox labeled "Enable UPnP Service" which is checked. At the bottom right of the configuration area, there is an "APPLY" button.

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.



The screenshot shows a web interface with two tabs: "UPNP DISCOVERY SERVICE" and "BONJOUR". The "BONJOUR" tab is active. Below the tabs, the heading "Bonjour" is displayed. A message states: "Before broadcasting the following services through Bonjour, please DO NOT forget to enable these services first." Below this message is a "Select all" checkbox, which is checked. A list of services follows, each with a checked checkbox and a "Service Name" input field:

- Web Administration
Service Name:
- SAMBA (Server Message Block over TCP/IP)
Service Name:
- AFP (Apple File Protocol over TCP/IP)
Service Name:
- SSH
Service Name:
- FTP (File Transfer Protocol)
Service Name:
- HTTPS (Secure web server)
Service Name:
- DLNA Media Server
Service Name:

7. Applications

Web File Manager [314](#)

Multimedia Station [332](#)

Photo Station [387](#)

Music Station [413](#)

Music Station [437](#)

Download Station [459](#)

Surveillance Station [487](#)

iTunes Server [490](#)

DLNA Media Server [493](#)

MySQL Server [494](#)

QPKG Center [496](#)

Syslog Server [500](#)

RADIUS Server [503](#)

Backup Server [509](#)

Antivirus [513](#)

TFTP Server [523](#)

VPN Service [524](#)

LDAP Server [540](#)

7.1 Web File Manager

The Web File Manager allows the users to access the NAS on the Internet and manage the files by a web browser. Enable the service in "Administration" > "Applications" > "Web File Manager". Click the link on the page to access the Web File Manager.

Home >> Application Servers >> Web File Manager Welcome admin | Logout English

Web File Manager

Web File Manager

- Enable Web File Manager
 - Show service link on the login page

After enabling this service, click the following link to enter to Web File Manager.

<http://10.8.13.59:8080/cgi-bin/filemanager/>

<https://10.8.13.59:443/cgi-bin/filemanager/>

APPLY

You can upload, download, rename, move, copy, or delete the files and folder on the NAS.

The screenshot displays the QNAP Web File Manager interface. The top navigation bar includes the QNAP logo, the text "WEB FILE MANAGER", and a user status area with "Welcome admin | Logout" and "English". The left sidebar shows a tree view of the file system with "Usb" selected. The main content area shows a table of files and folders in the "/Usb" directory.

Name	Size	Type	Modified Time	Permission	Owner	Group
AA		Folder	2011/11/14 17:34:08	770 (rwxrwx--)	admin	administrators

At the bottom of the interface, there is a pagination control showing "Page 1 / 1" and a "Disk info" section reporting "Used Size : 123.84 GB , Free Size : 167.6 GB".

Upload files

Note: The maximum size of a file that can be uploaded to the NAS by the 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.

Upload destination: /Public/pic

Files to be uploaded:(2) Total size: 184.9 KB **Uploaded files(0) Total size: 0 B**

	Mode	Name	Size	%	Transfer Rate	Time Remaining
 	-	Winter.jpg	103.07 KB	0%	0 B/Sec.	
 	-	Water lilies.jpg	81.83 KB	0%	0 B/Sec.	

If the file already exists: Skip Overwrite

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

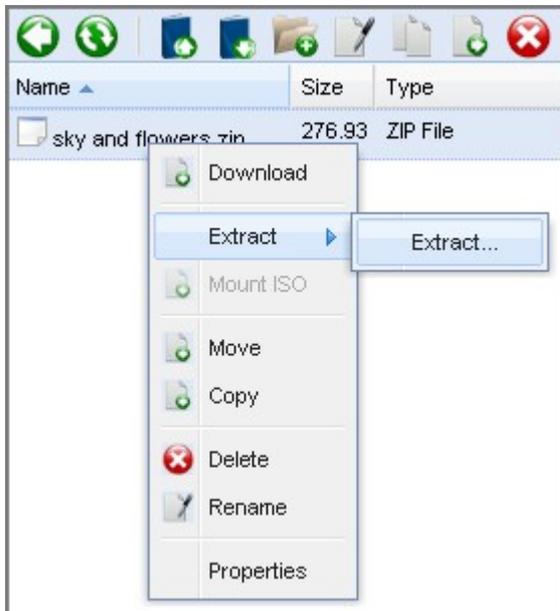
- i. Select the files or folders to move.
- ii. Click  (Move).
- iii. Select the destination folder.
- iv. Select to skip or overwrite the existing file in the destination folder. Click "OK".

Delete file or folder

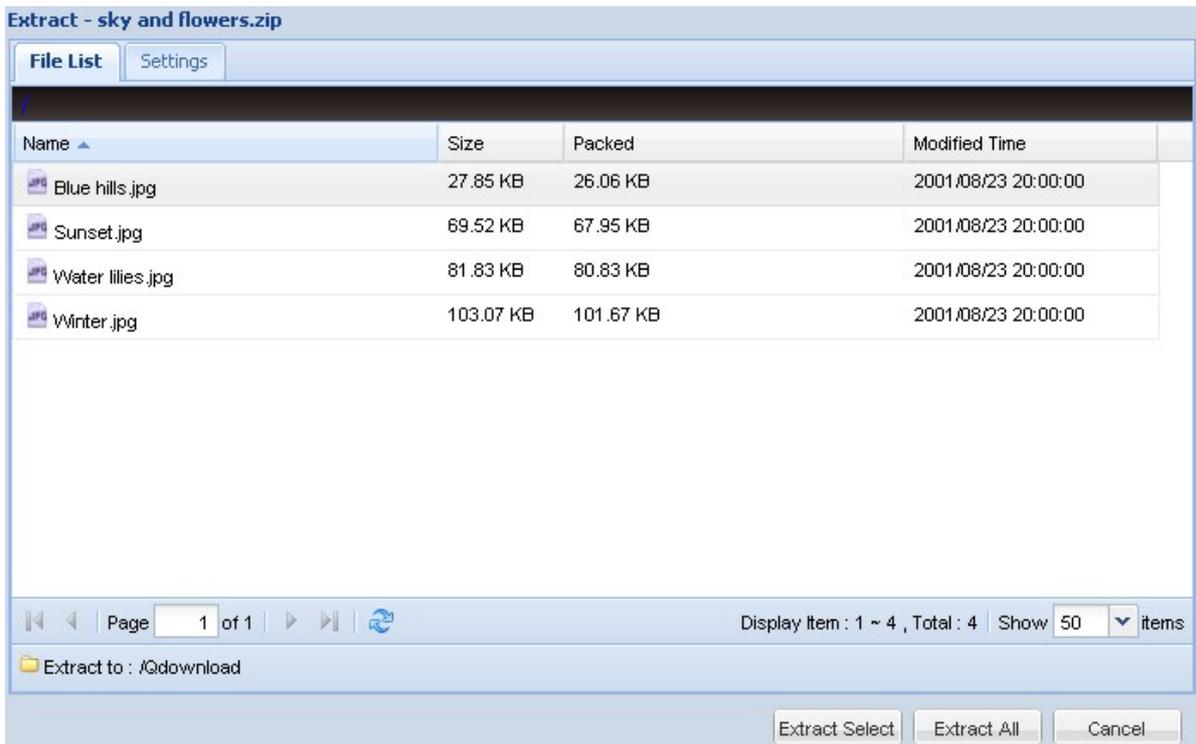
- i. Select a file or folder to delete.
- ii. Click  (Delete) on the toolbar.
- iii. Confirm to delete the file or folder.

Extract files

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

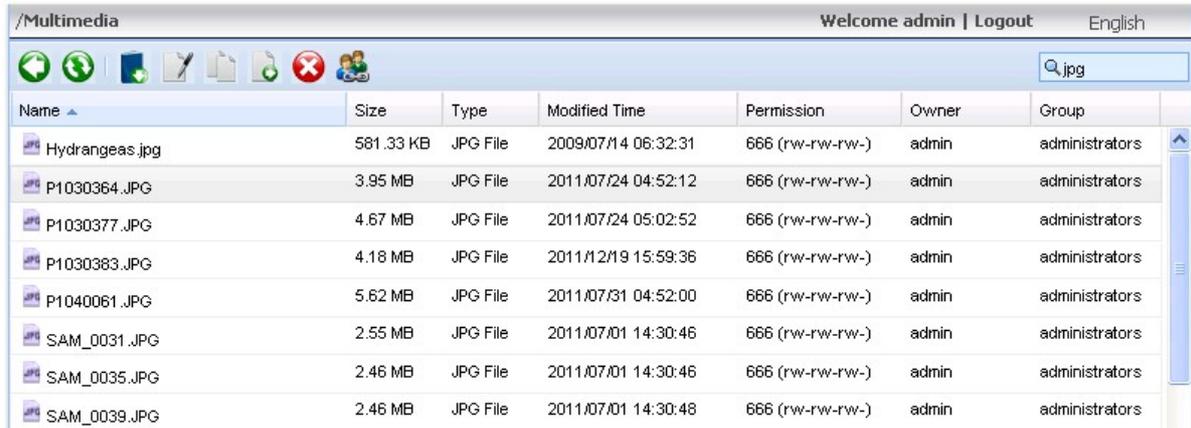


ii. Select the files to extract and configure the extraction settings.



Files/Folders Search

The 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.



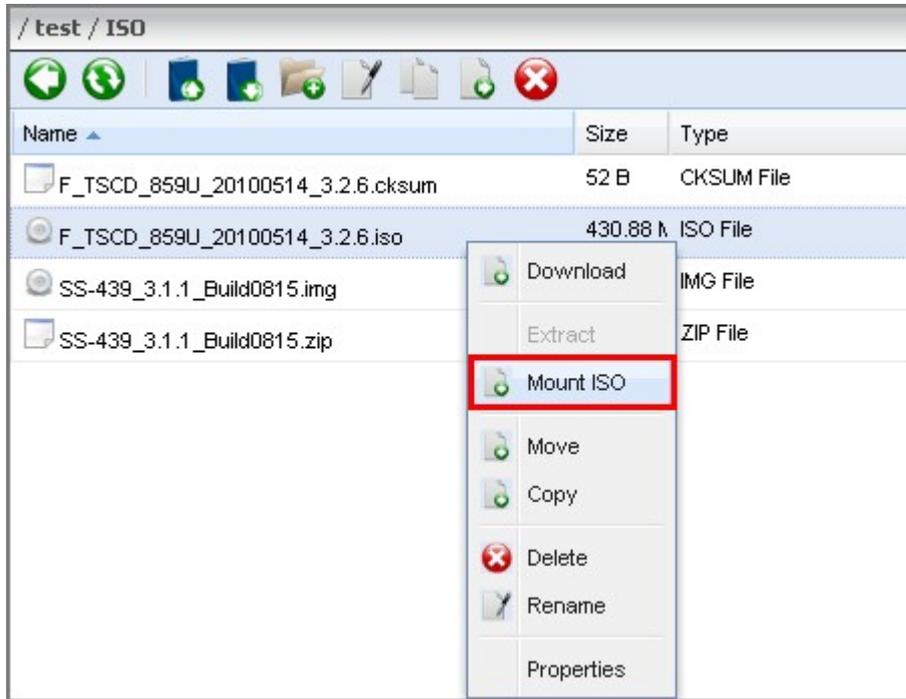
The screenshot shows a web interface for a file manager. At the top, it says "/Multimedia" on the left, "Welcome admin | Logout" in the center, and "English" on the right. Below this is a toolbar with various icons (back, forward, refresh, home, search, delete, etc.) and a search input field containing ".jpg". The main area is a table with the following columns: Name, Size, Type, Modified Time, Permission, Owner, and Group. The table lists eight files, all of which are JPG files owned by 'admin' and belonging to the 'administrators' group.

Name	Size	Type	Modified Time	Permission	Owner	Group
Hydrangeas.jpg	581.33 KB	JPG File	2009/07/14 06:32:31	666 (rw-rw-rw-)	admin	administrators
P1030364.JPG	3.95 MB	JPG File	2011/07/24 04:52:12	666 (rw-rw-rw-)	admin	administrators
P1030377.JPG	4.67 MB	JPG File	2011/07/24 05:02:52	666 (rw-rw-rw-)	admin	administrators
P1030383.JPG	4.18 MB	JPG File	2011/12/19 15:59:36	666 (rw-rw-rw-)	admin	administrators
P1040061.JPG	5.62 MB	JPG File	2011/07/31 04:52:00	666 (rw-rw-rw-)	admin	administrators
SAM_0031.JPG	2.55 MB	JPG File	2011/07/01 14:30:46	666 (rw-rw-rw-)	admin	administrators
SAM_0035.JPG	2.46 MB	JPG File	2011/07/01 14:30:46	666 (rw-rw-rw-)	admin	administrators
SAM_0039.JPG	2.46 MB	JPG File	2011/07/01 14:30:48	666 (rw-rw-rw-)	admin	administrators

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".



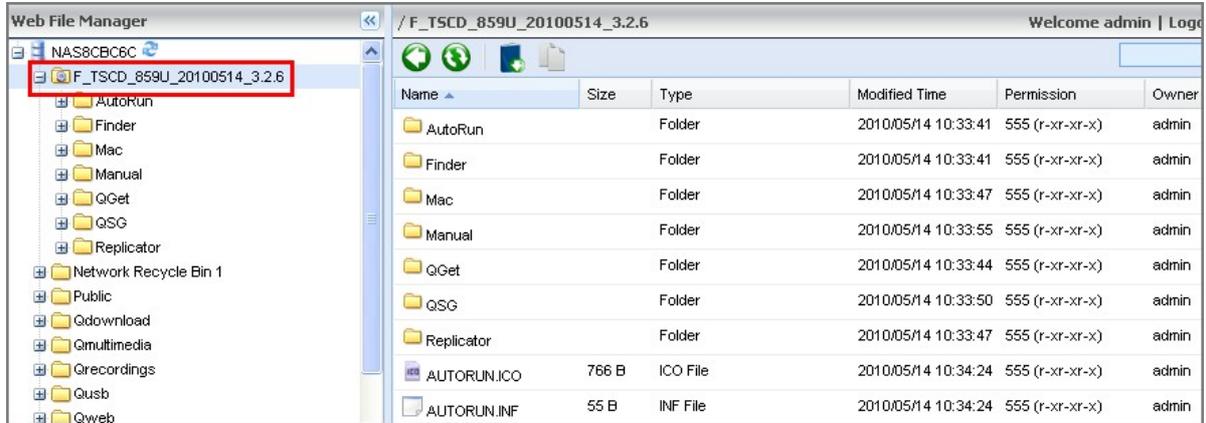
Enter the share name and click "OK".



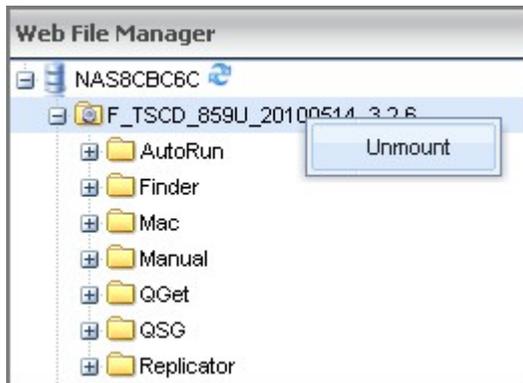
Click "OK" to confirm.



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".

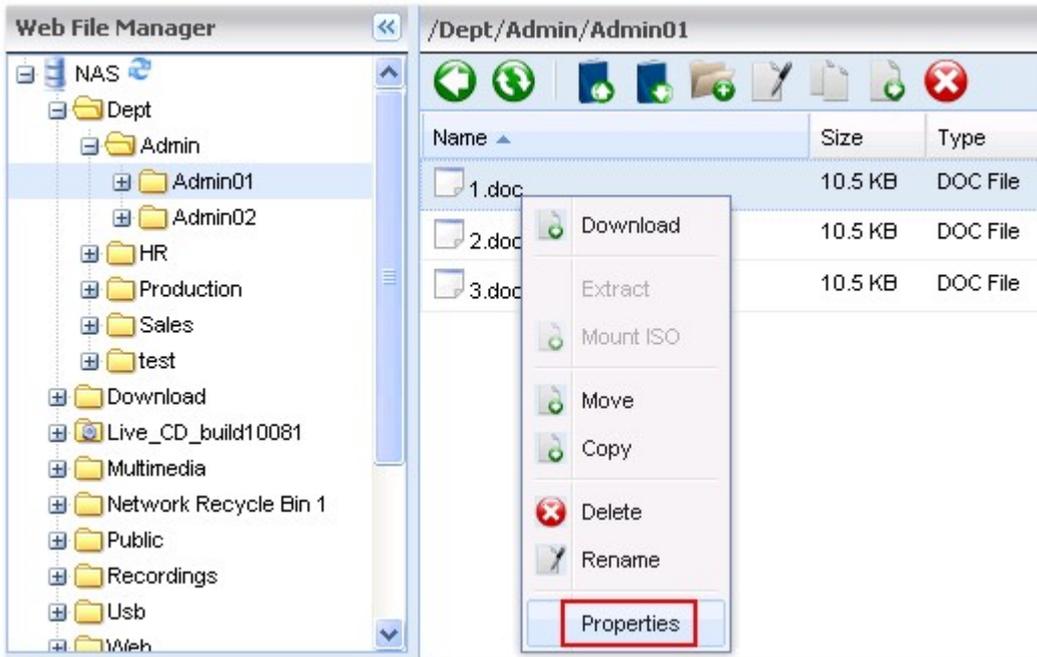


To unmount the share, right click the folder name and select "Unmount". Click "Yes" to confirm and then click "OK" to unmount.



File/Folder Level Permissions

You can set file or folder level permissions on the NAS by the 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.

The screenshot shows a 'Properties' dialog box with two main sections: 'Info' and 'Permission'. The 'Info' section displays the following details: Name: 1.doc, Location: /Dept/Admin/Admin01, Size: 10.5 KB, and Modified Time: 2011/01/19 09:15:54. The 'Permission' section is a table with columns for 'Read', 'Write', and 'Execute' and rows for 'Owner', 'Group', and 'Public'. Each cell contains a checkbox, which is checked for Owner, Group, and Read/Write for Public, but unchecked for Public's Execute permission. At the bottom right, there are 'OK' and 'Cancel' buttons.

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

Properties

Info

Name : Admin01
Location : /Dept/Admin
Size : 31.5 KB
Modified Time : 2011/01/19 09:16:12

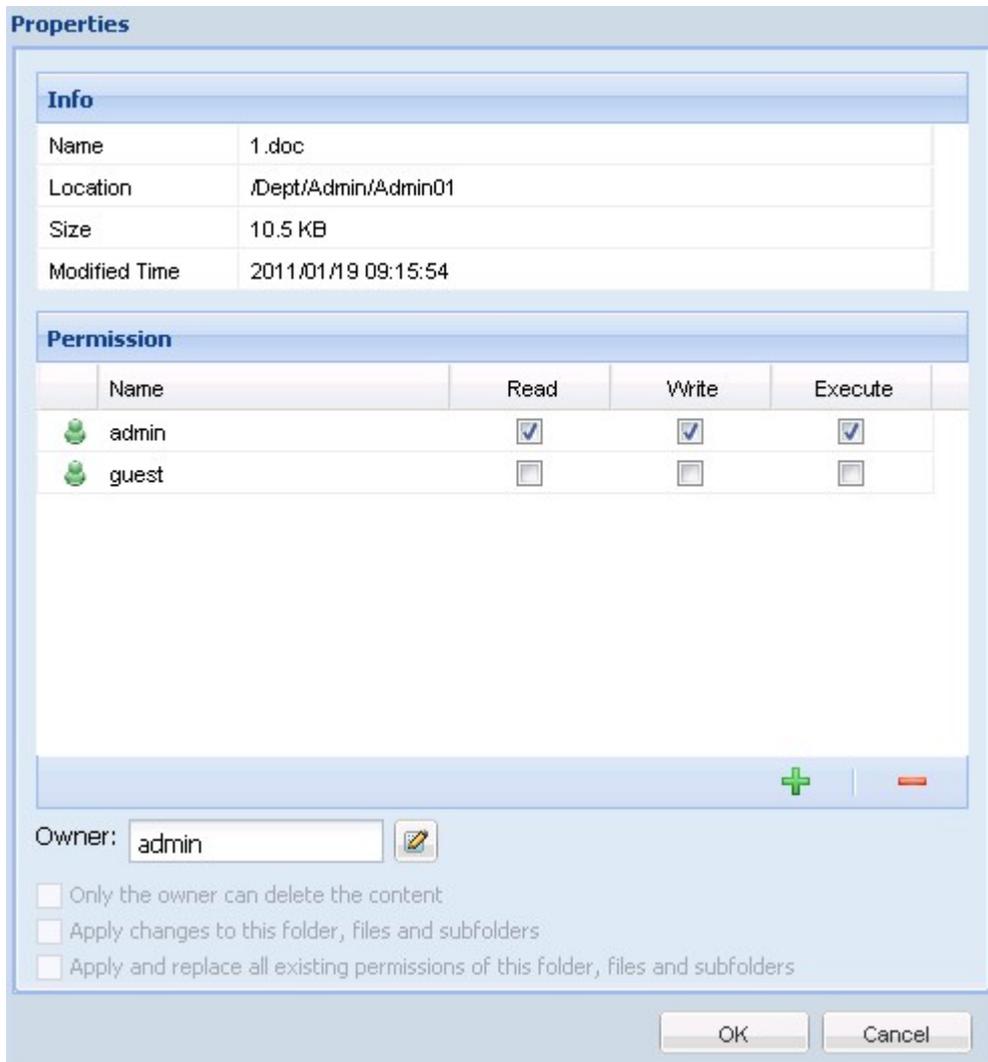
Permission

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply changes to the folder(s), subfolder(s) and file(s)

OK Cancel

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 .



The image shows a Windows 'Properties' dialog box for a file named '1.doc'. The 'Info' tab is active, displaying the file's location as '/Dept/Admin/Admin01', size as '10.5 KB', and modified time as '2011/01/19 09:15:54'. The 'Permission' tab is also visible, showing a table of permissions for 'admin' and 'guest' users. The 'admin' user has Read, Write, and Execute permissions checked, while the 'guest' user has all three unchecked. Below the table, there is a green plus icon and a red minus icon. At the bottom, the 'Owner' is set to 'admin', and there are three checkboxes: 'Only the owner can delete the content', 'Apply changes to this folder, files and subfolders', and 'Apply and replace all existing permissions of this folder, files and subfolders'. The 'OK' and 'Cancel' buttons are at the bottom right.

Name	Read	Write	Execute
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Select users and groups

Local Users

<input type="checkbox"/> Name	Read	Write	Execute
<input checked="" type="checkbox"/> test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Alex	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> test1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> test2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> test1 234	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> jauss	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> testsss	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Page 1 / 1 Display Item : 1 ~ 7 , Total : 7

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

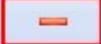
Properties

Info

Name	1.doc
Location	./Dept/Admin/Admin01
Size	10.5 KB
Modified Time	2011/01/19 09:15:54

Permission

Name	Read	Write	Execute
 admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 test	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 test1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 test2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner: 

Only the owner can delete the content
 Apply changes to this folder, files and subfolders
 Apply and replace all existing permissions of this folder, files and subfolders

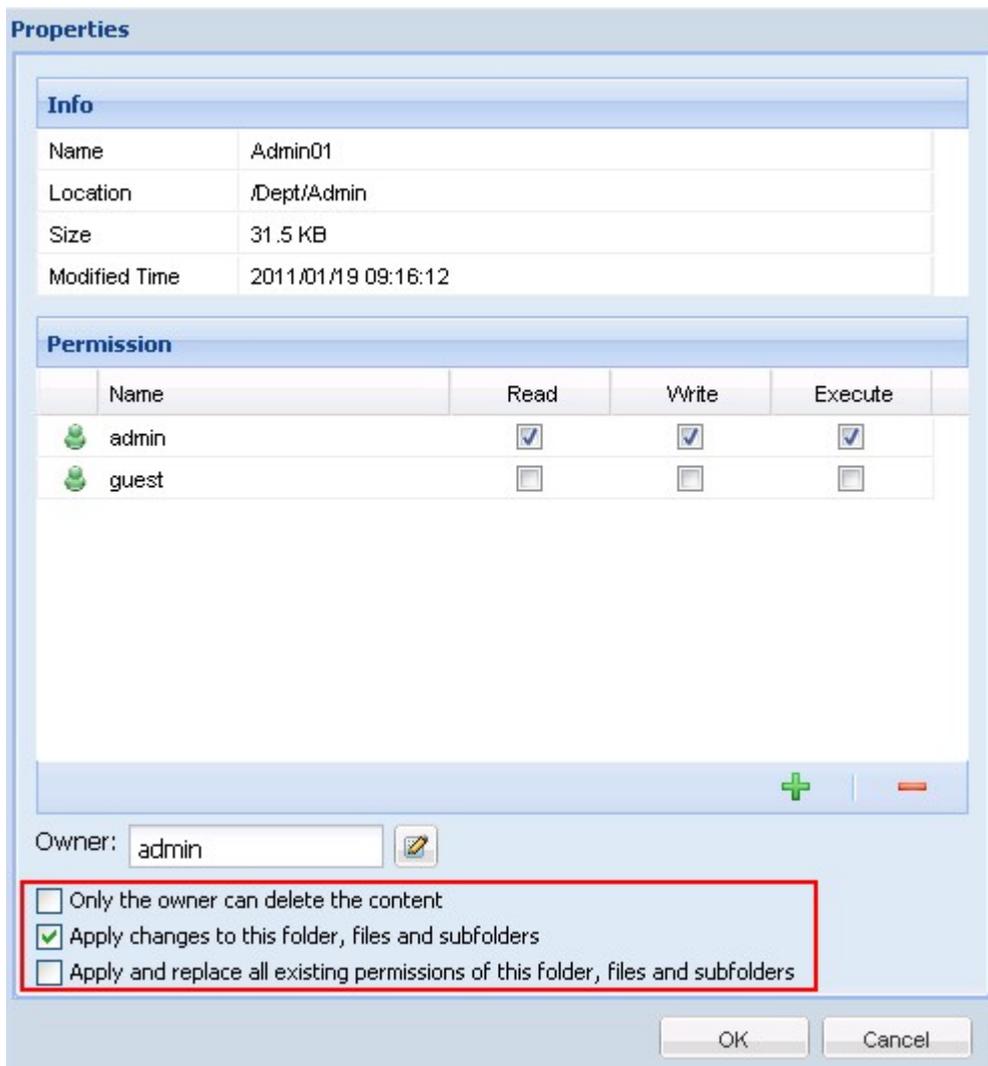
OK Cancel

You can also define the file and folder owner by clicking . Select a user from the list or search a username. 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"²³⁶.

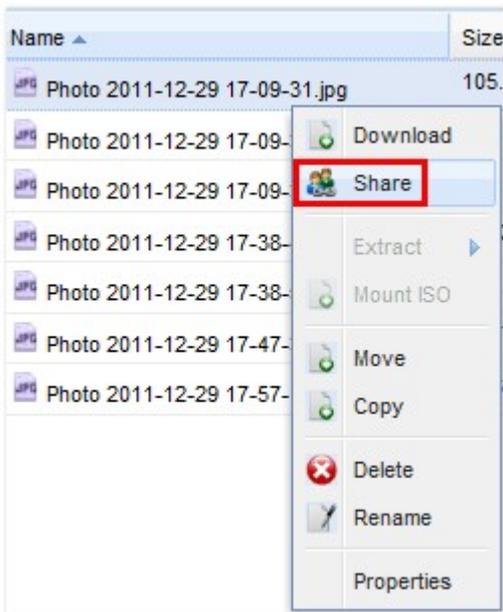
- Only the owner can delete the contents: When you apply this option to a folder, the first-level subfolders and files can be deleted only by their owner.
- Apply changes to files and subfolders: Apply changed permissions settings except owner protection to all the files and subfolders within the selected 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.



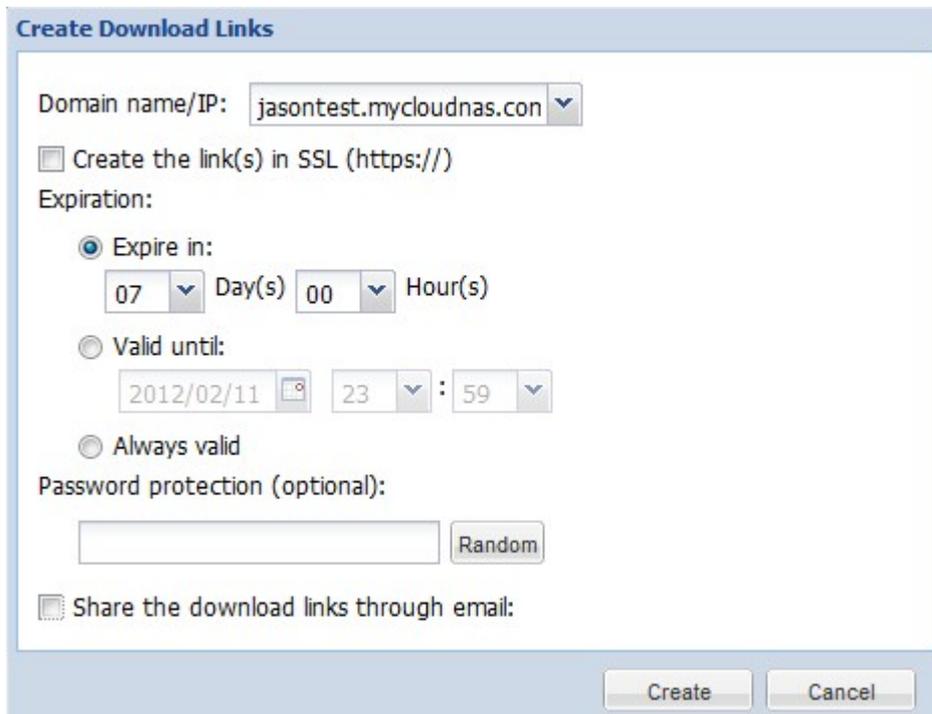
Share Files

Note: This feature can only be used by admin.

To share the files on the NAS by the 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).

A screenshot of a dialog box titled "Create Download Links". It contains the following fields and options:

- Domain name/IP: (dropdown arrow)
- Create the link(s) in SSL (https://)
- Expiration:
 - Expire in:
 - Day(s) Hour(s)
 - Valid until:
 - :
 - Always valid
- Password protection (optional):
 -
 -
- Share the download links through email:

At the bottom are "Create" and "Cancel" buttons.

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".

Share the download links through email:

Include the password

To:

Subject:

Content:

***Note:** Separate the email addresses by comma (,) or a semi-colon (;). Up to 5 email addresses can be sent.

Confirm the information and click "Start Sharing".

Sharing Links

Please confirm the following information

1. Photo 2011-12-29 17-09-31.jpg
<http://mcna.mycloudnas.com:8080/cgi-bin/filemanager/utilRequest.cgi?ssid=0NAS9nKM84>

Period of validity: 02/18/2012 23:56

7.2 Multimedia Station

The Multimedia Station is a web-based application for viewing the photos, playing music and videos on the NAS by a web browser, and sharing files to popular social networking sites such as Facebook, Plurk, Twitter, Blogger, and so on.

To use the Multimedia Station, follow the steps below.

1. Go to "Administration" > "Network Services" > "Web Server". Turn on the web server feature. To allow access to the Multimedia Station by HTTPS, turn on the option "Enable Secure Connection (SSL)".
2. Go to "Administration" > "Applications" > "Multimedia Station". Enable the service.
3. 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.

Multimedia Station

Enable Multimedia Station

After enabling this service, you may click one of the following links to enter Multimedia Station.

<http://10.8.13.59:80/MSV2/>

<https://10.8.13.59:8081/MSV2/>

Rescan media library

Daily start time: 00 : 00

The administrator accounts (admin) for local NAS administration and the application are the same. Please login as "admin".

Select either "System Users" or "Standalone Application Users" as the user accounts for the application. If "System User" is selected, set up the users and the access rights in "Access Right Management" > "Users". Otherwise, go to the application's page to set up the user accounts.

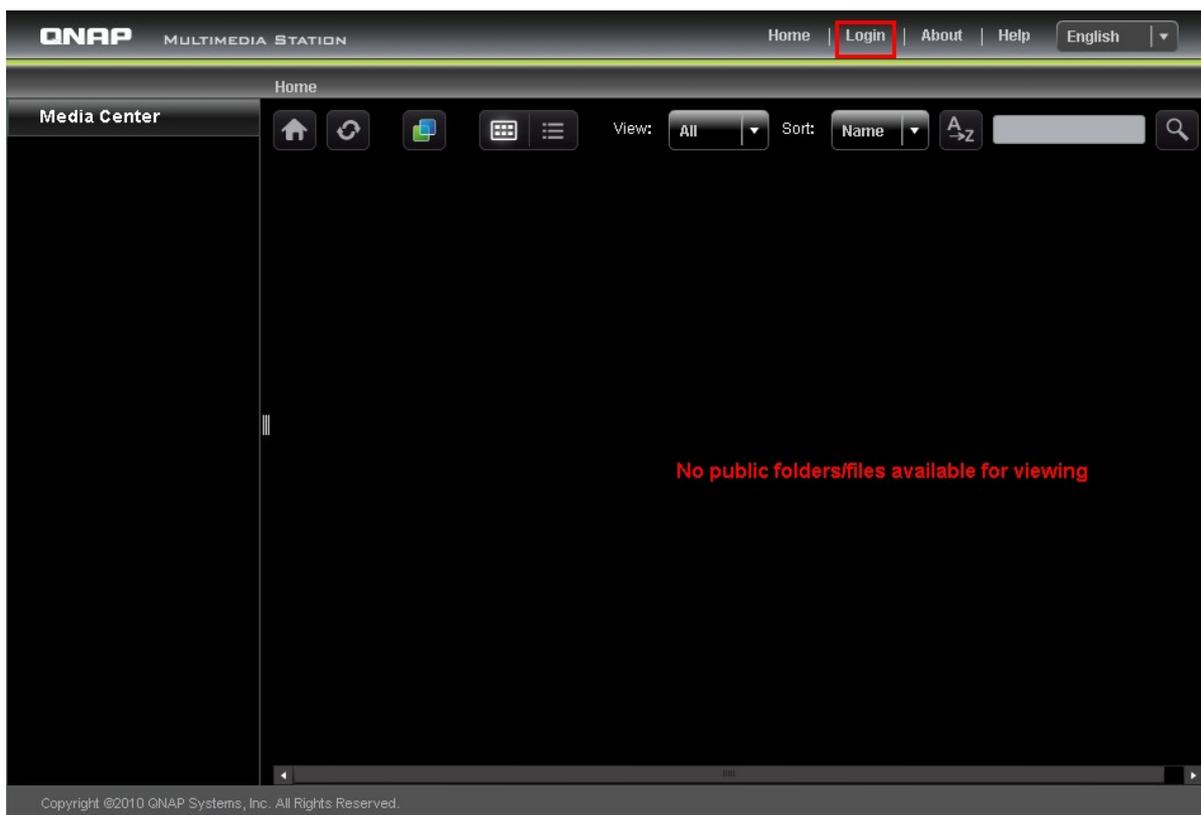
User Account Settings: Standalone Application Users

APPLY

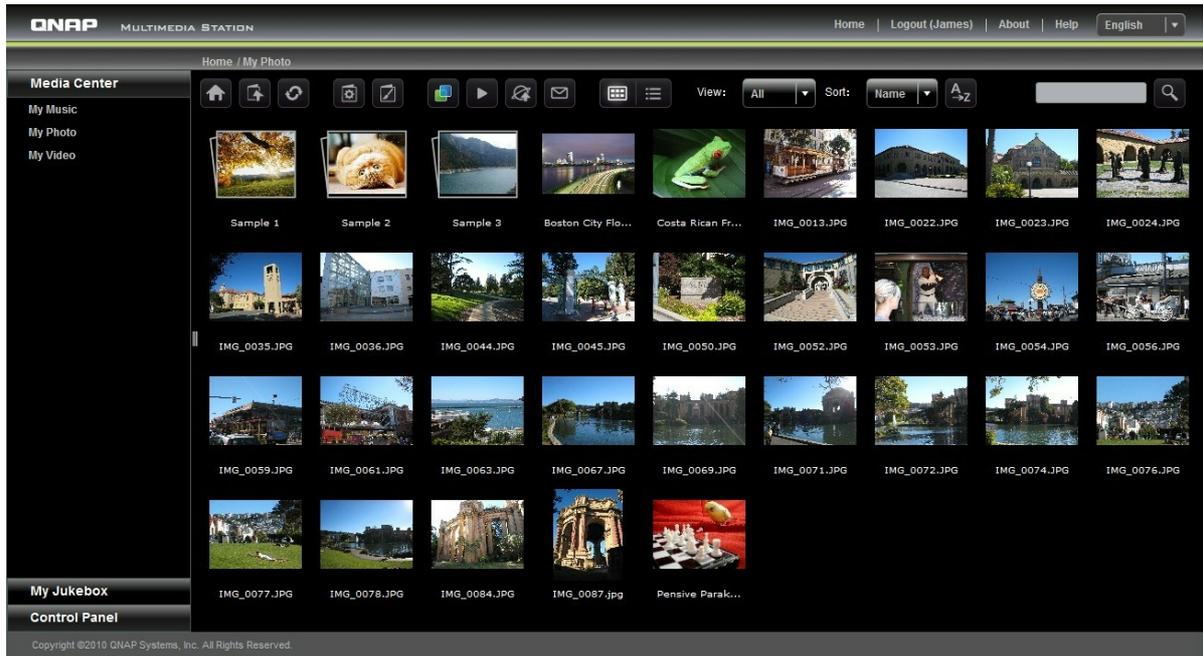
4. Select either "System Users" or "Standalone Application Users" (default) for the user account settings. When "System Users" is selected, the local NAS accounts will be used for the application. You can create the user accounts in "Access Right Management" > "Users". To use dedicated user accounts for the application, select "Standalone Application Users". The user accounts can be created and managed after logging in the application under "Control Panel" > "User Management".
5. Connect to the Multimedia Station from the login portal of the NAS or enter `http://NAS_IP:80/MSV2/` or `https://NAS_IP:8081/MSV2/` (secure connection) in a web browser. Login the application when you are prompted to. Only the administrator (admin) can create users and configure the advanced settings.

Note:

- The admin login information of the Multimedia Station is the same as that of the NAS web administration.
- Login to the application from the login portal page of the NAS will be disabled when standalone user accounts are in use, except for "admin".



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



Media Center

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

Supported file format

Type	File format
Audio	MP3
Image	JPG/JPEG, GIF, PNG (The 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 (The files will be converted to FLV.)



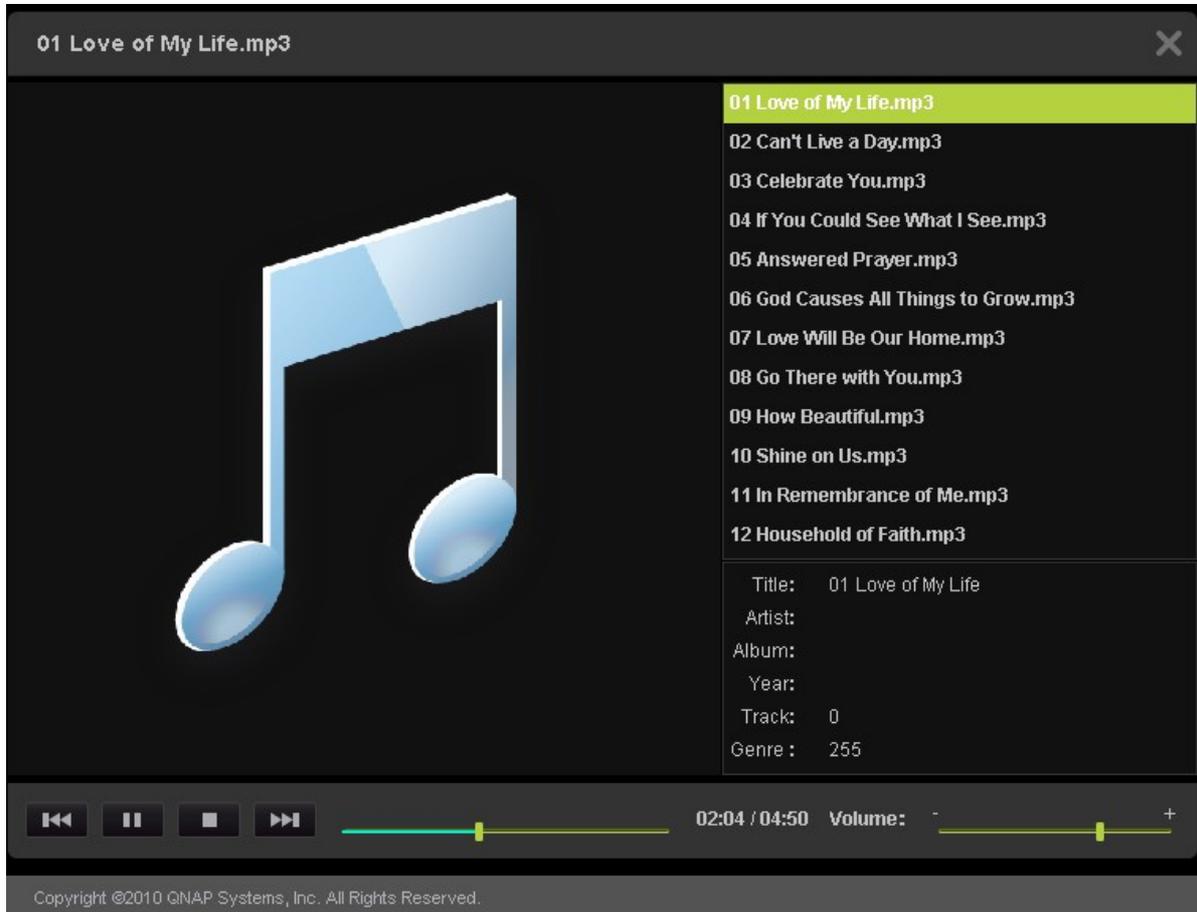
Icon	Description
	<p>Home</p> <p>Return to the home directory of the Multimedia Station.</p>
	<p>Parent Directory</p> <p>Return to the parent directory.</p>
	<p>Refresh</p> <p>Refresh the current directory.</p>
	<p>Manage Album*</p> <p>You can: 1. create albums under the current directory and 2. add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

	Browse the files in detailed view. It supports the functions: Open, Rename, Delete, Download, and Full Image View.
	Sort Sort the files alphabetically in ascending or descending order.
	Search Search files within the current directory.

*These features can only be operated by the administrator.

Play music

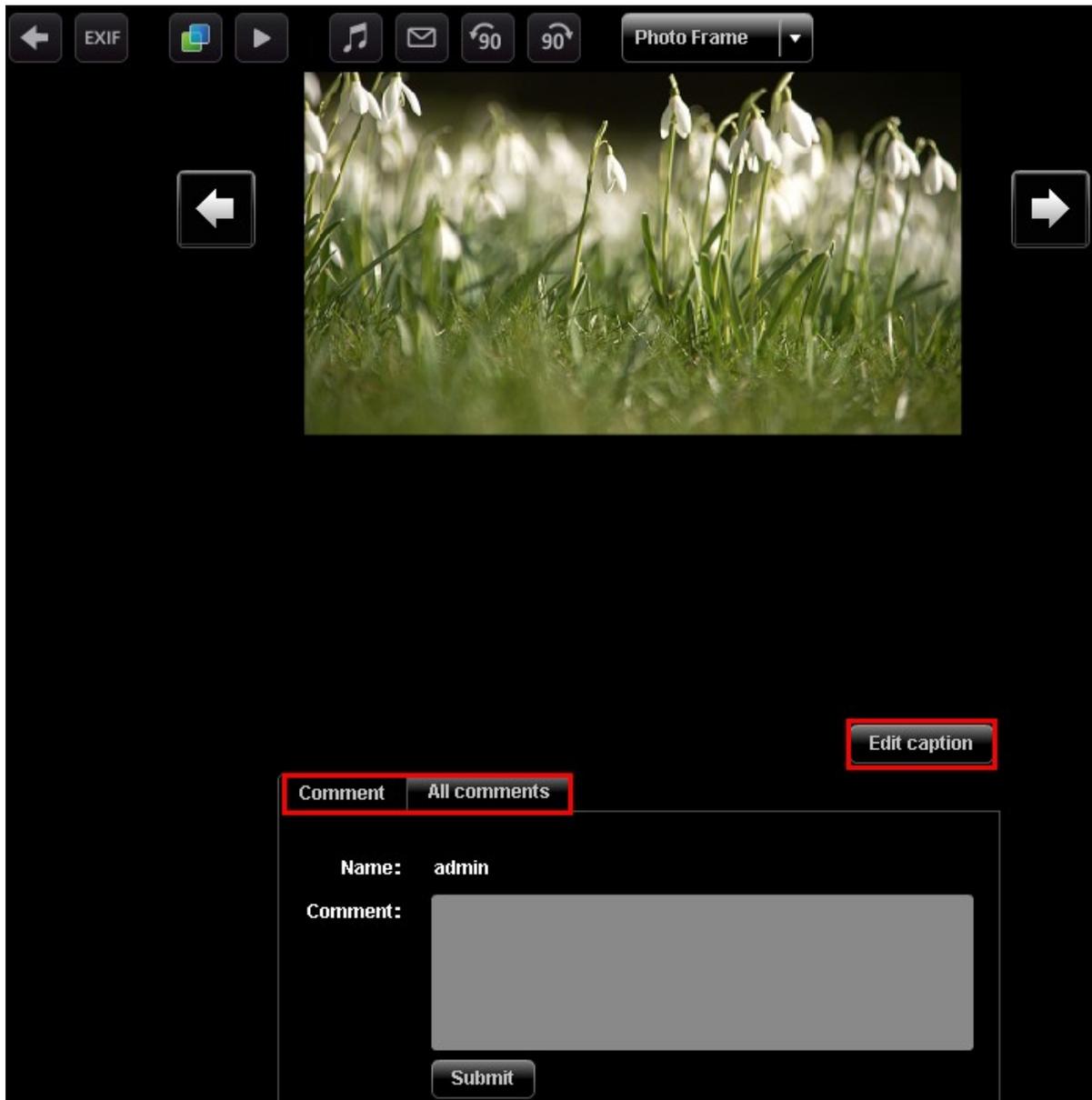
Click an MP3 file to play the music by a web browser. When you click a music file in a folder, all the other supported music files in the folder will also be added to the playlist. Click "X" to exit.



View image files

When viewing an image file, 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.

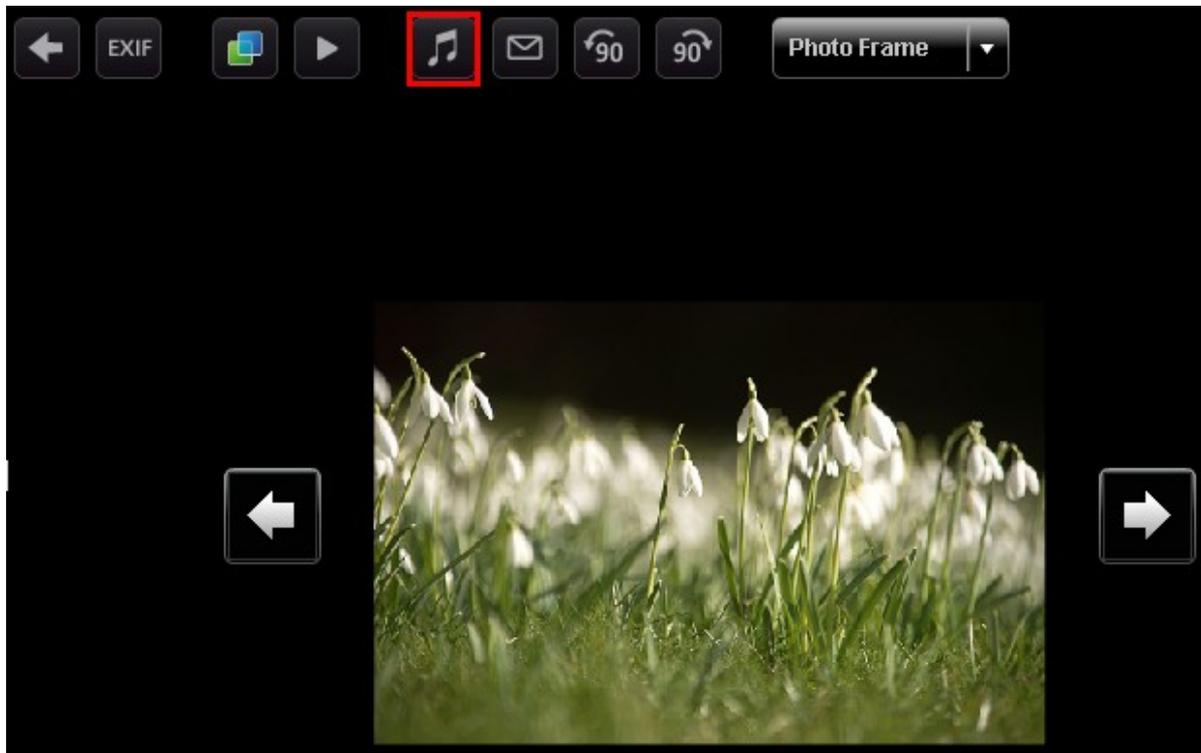
You can also submit your comments on the image file and view the comments from other users on "All comments". Each comment cannot exceed 128 characters.



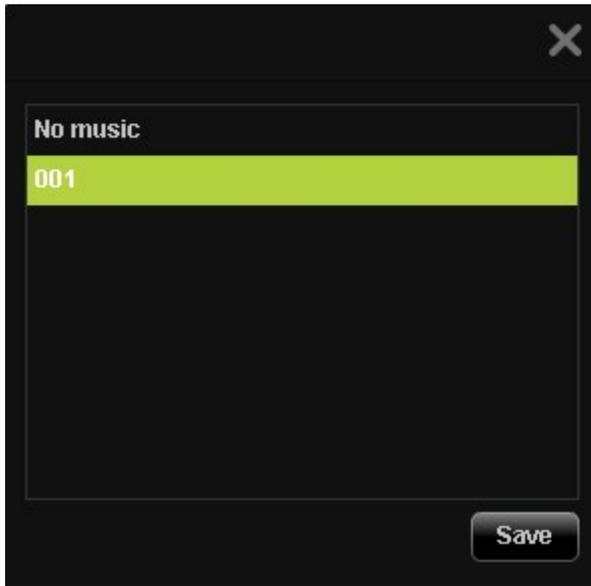
Set background music

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 the Multimedia Station.

Open an image file in Media Center and click .

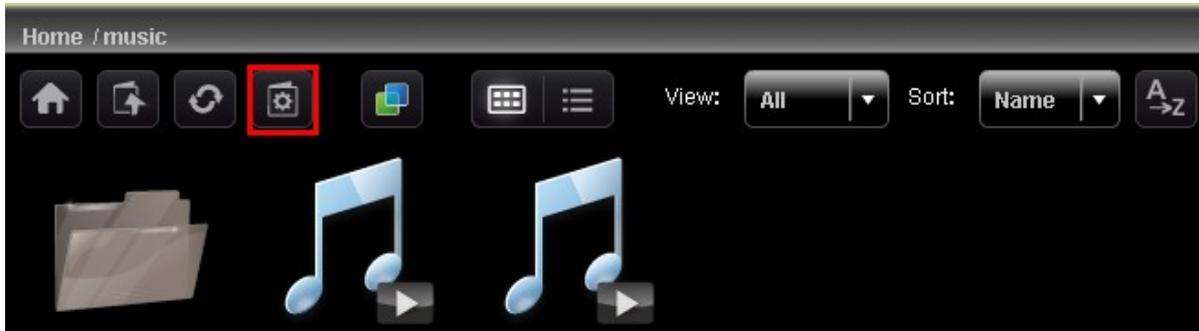


Select the playlist and click "Save". To remove the background music, you can select "No music".



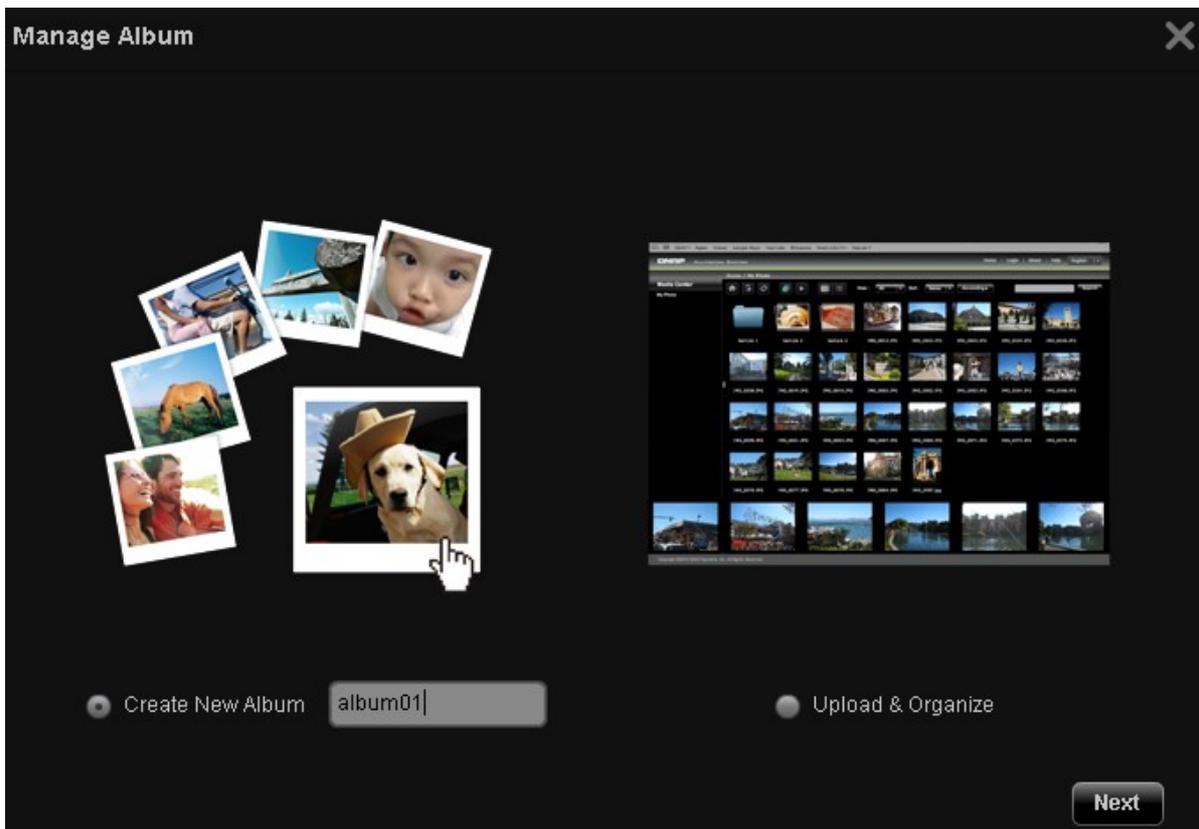
Create album

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

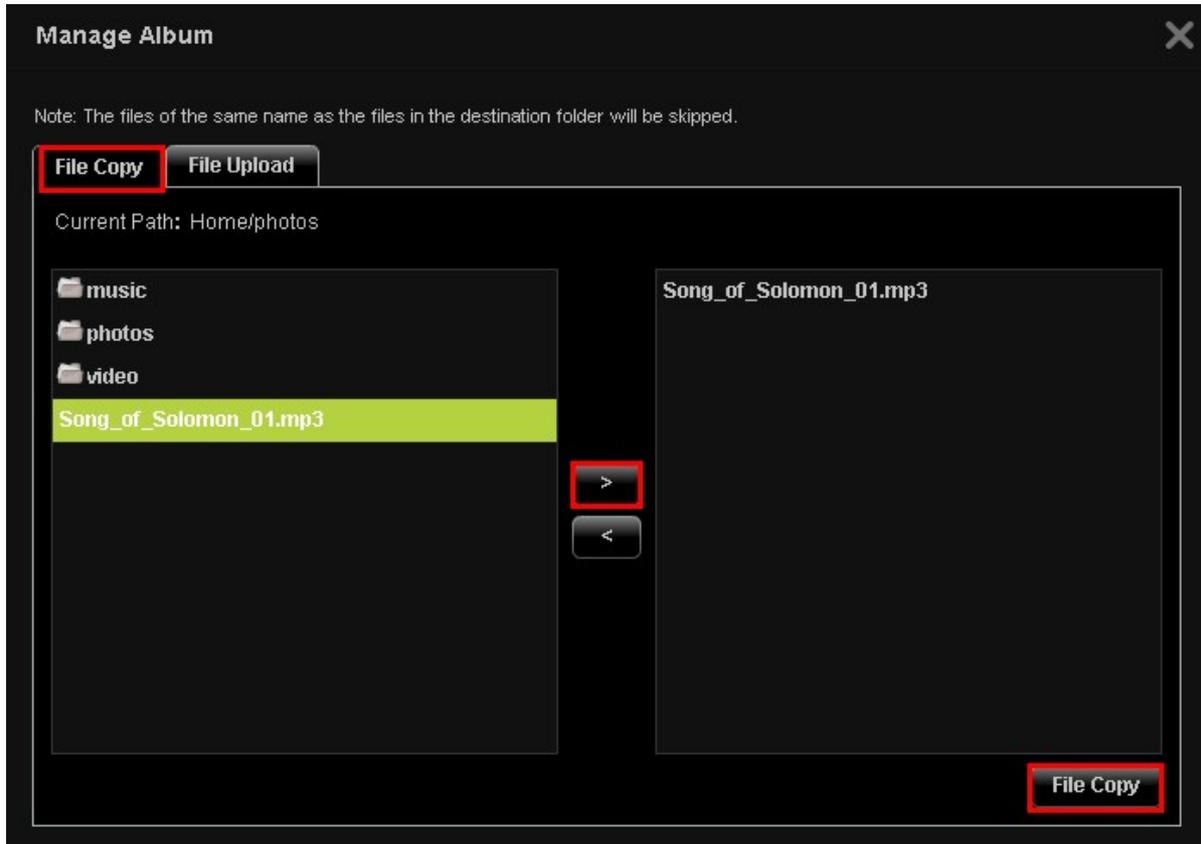


Select "Create New Album" and enter the album name. Click "Next".

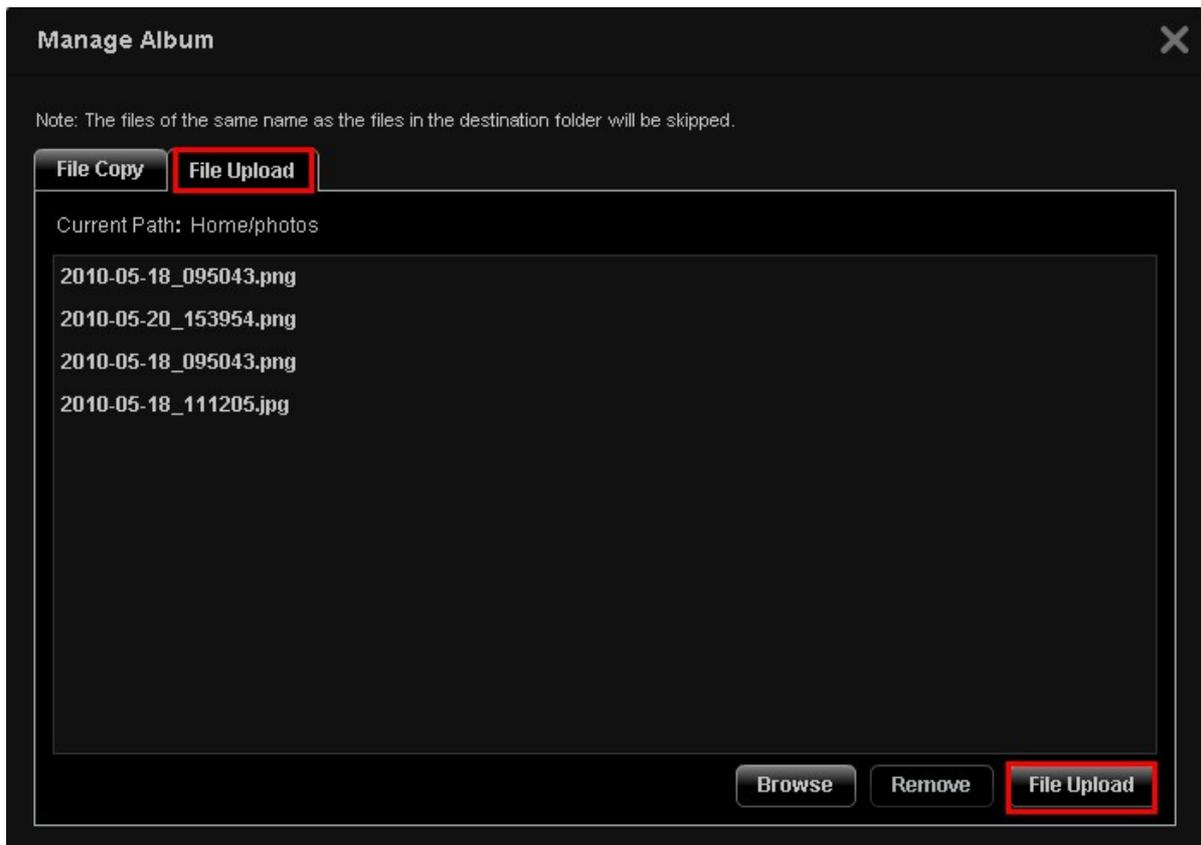
The album name must be 1 to 64 characters long, and cannot contain | \ : ? " < > *



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.

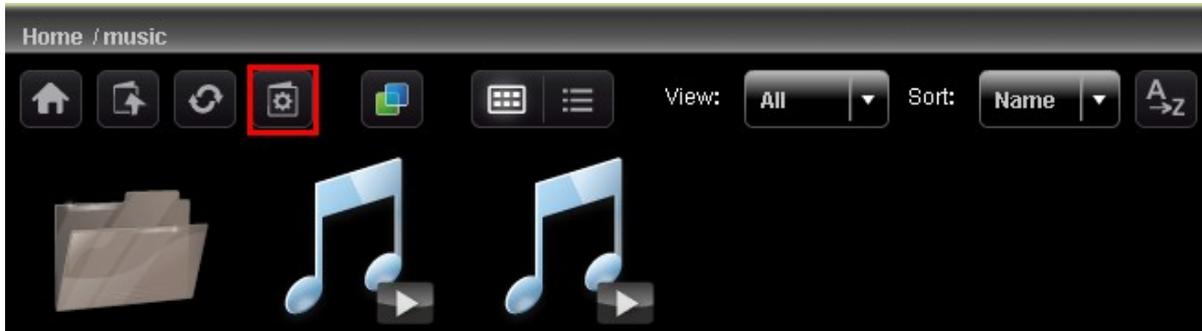


To upload files to the album, click "Browse" to select the files and click "File Upload".

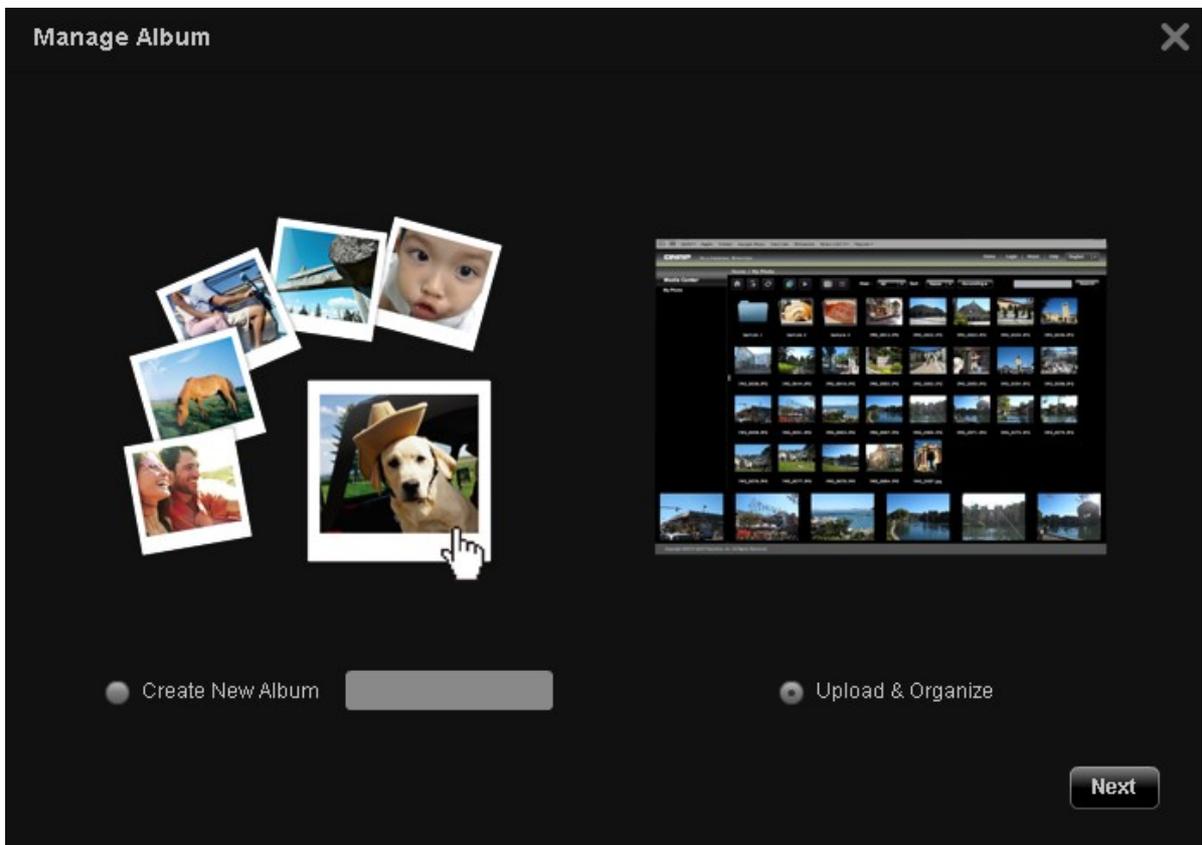


Manage album

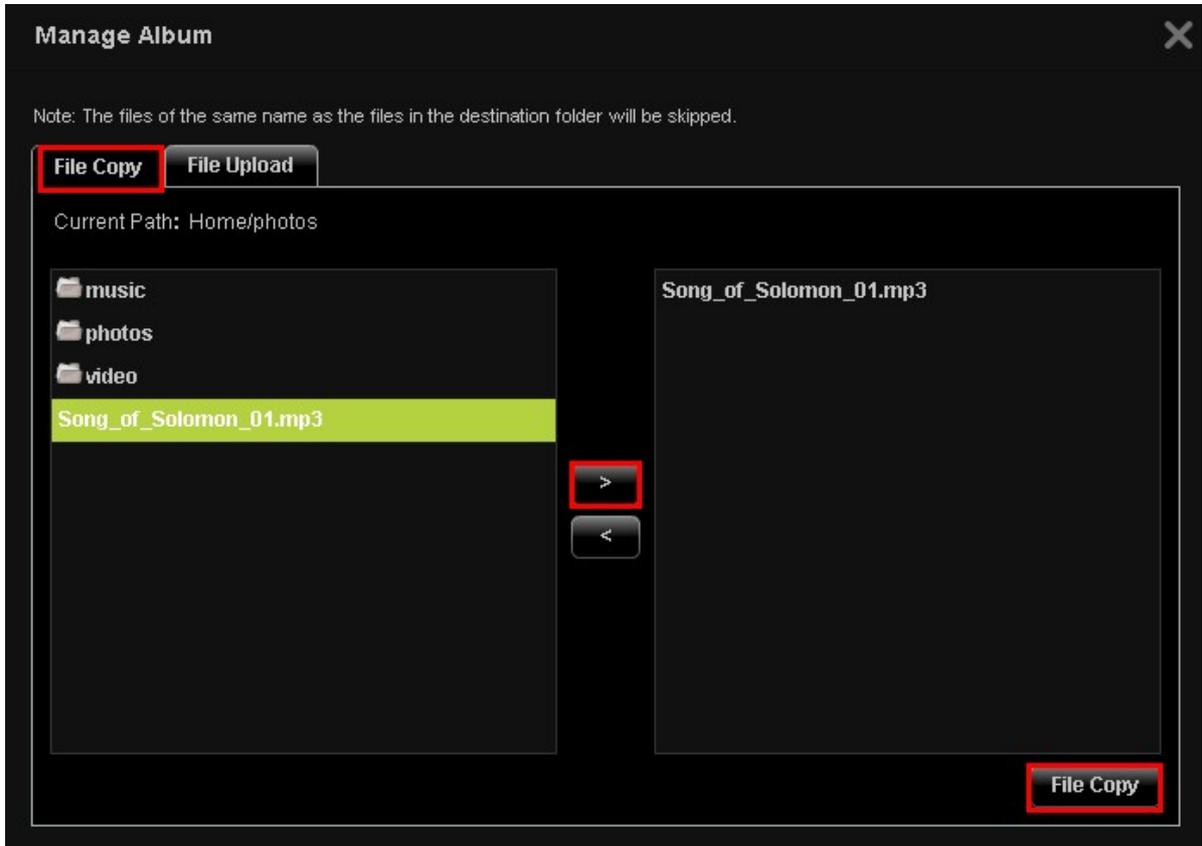
To manage an album (folder) by the web-based interface of the Multimedia Station, locate the directory in Media Center. Click  (Create Album).



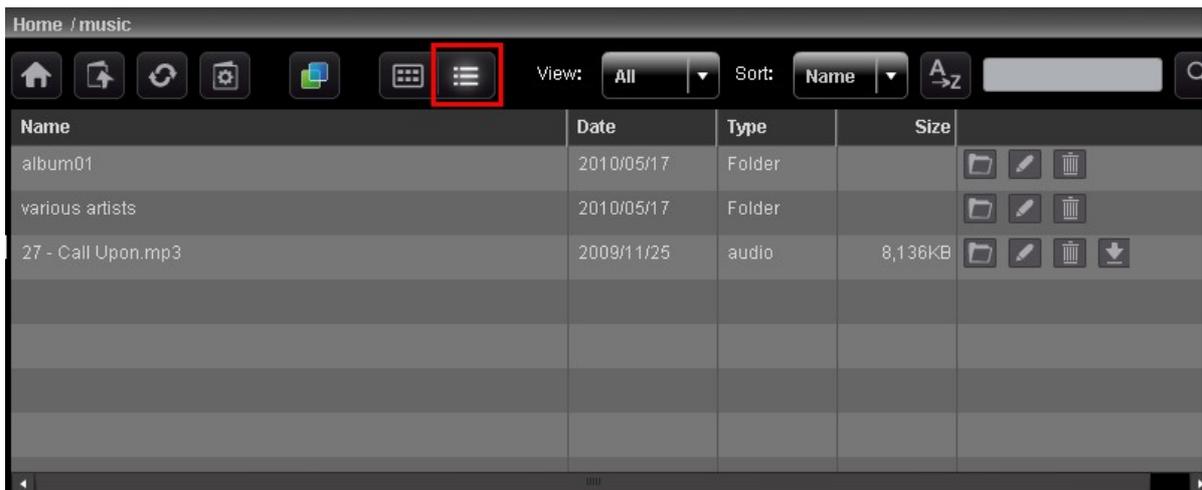
Select "Upload & Organize" and click "Next".



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".

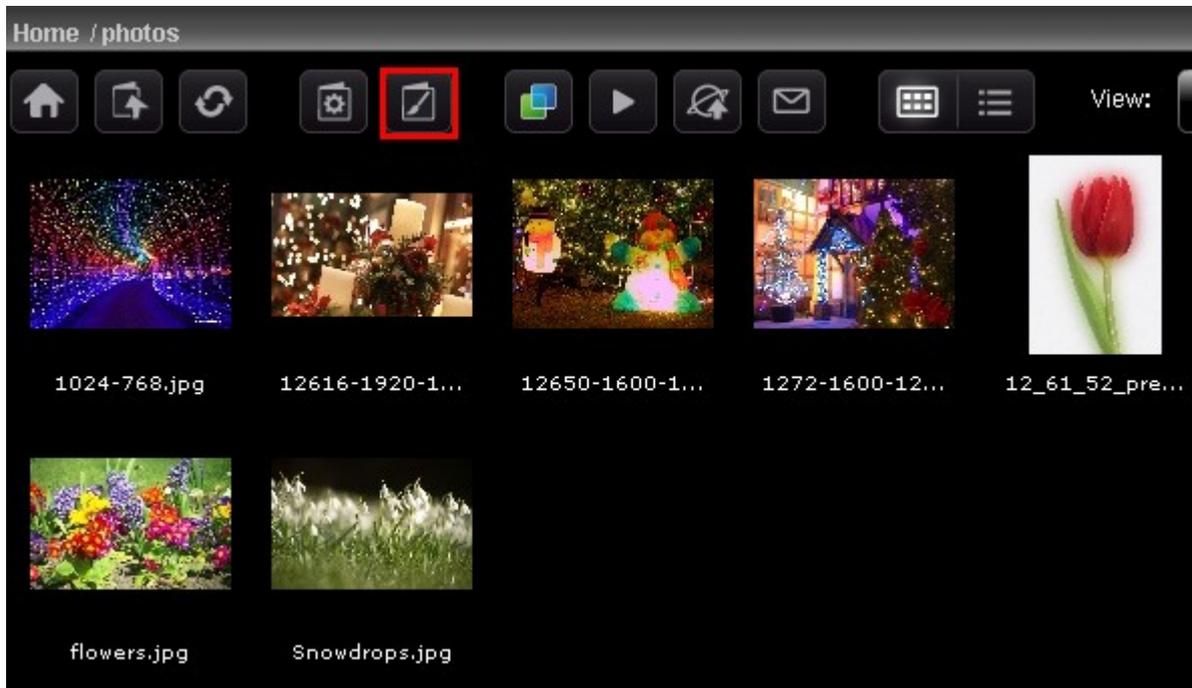


You can click  to browse the multimedia contents in details and click the icons to open, rename, delete, or download the files or folders.

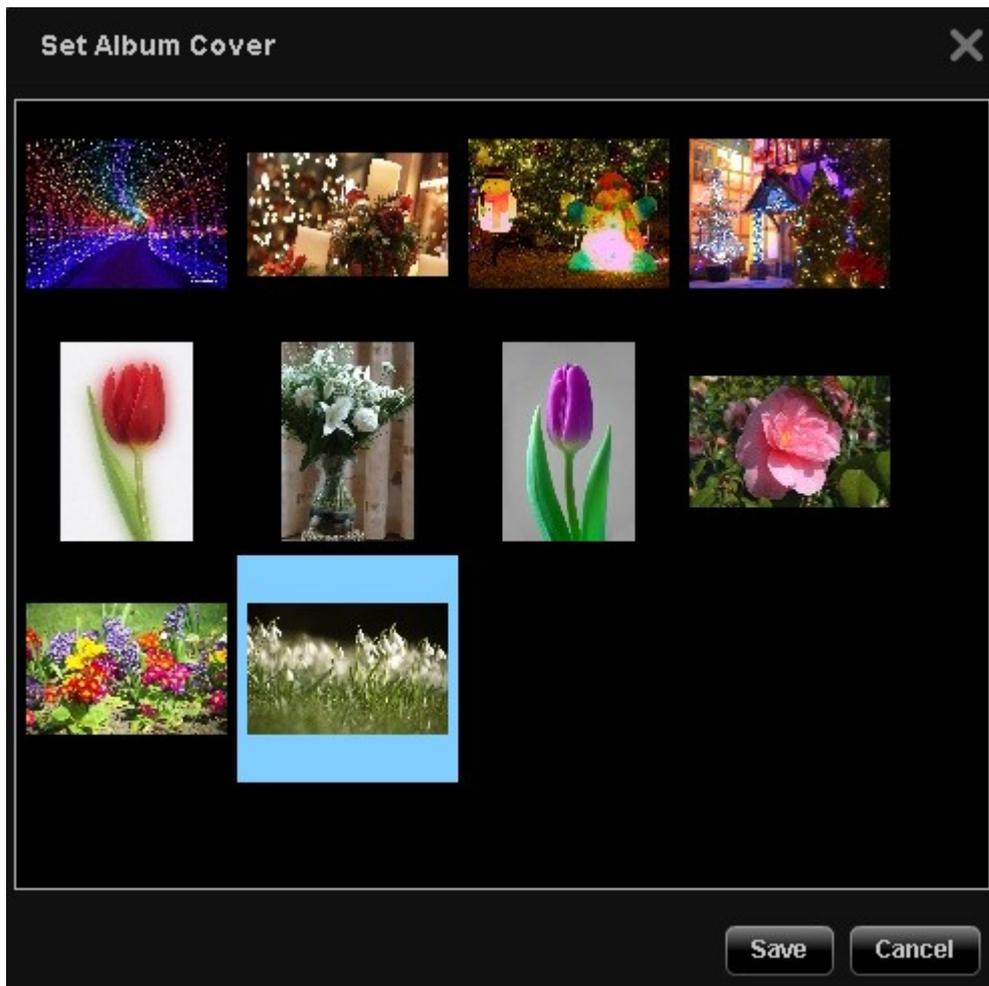


Set album cover

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



Select the image file and click "Save".

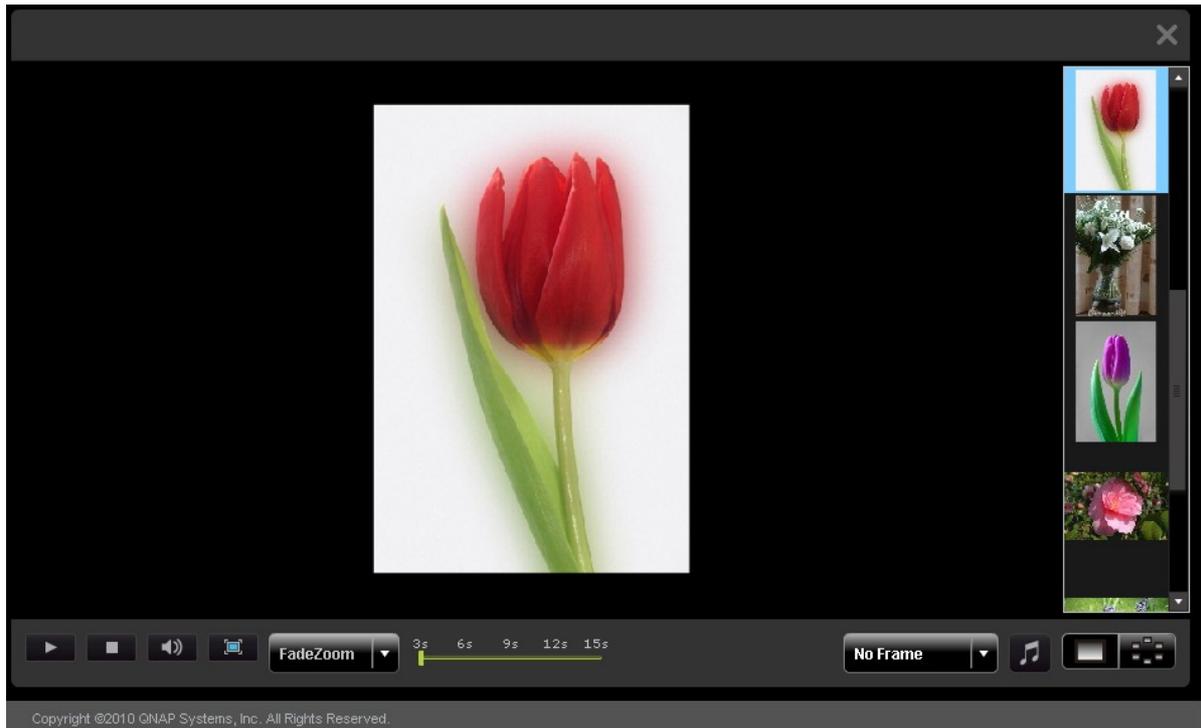


Slide Show



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

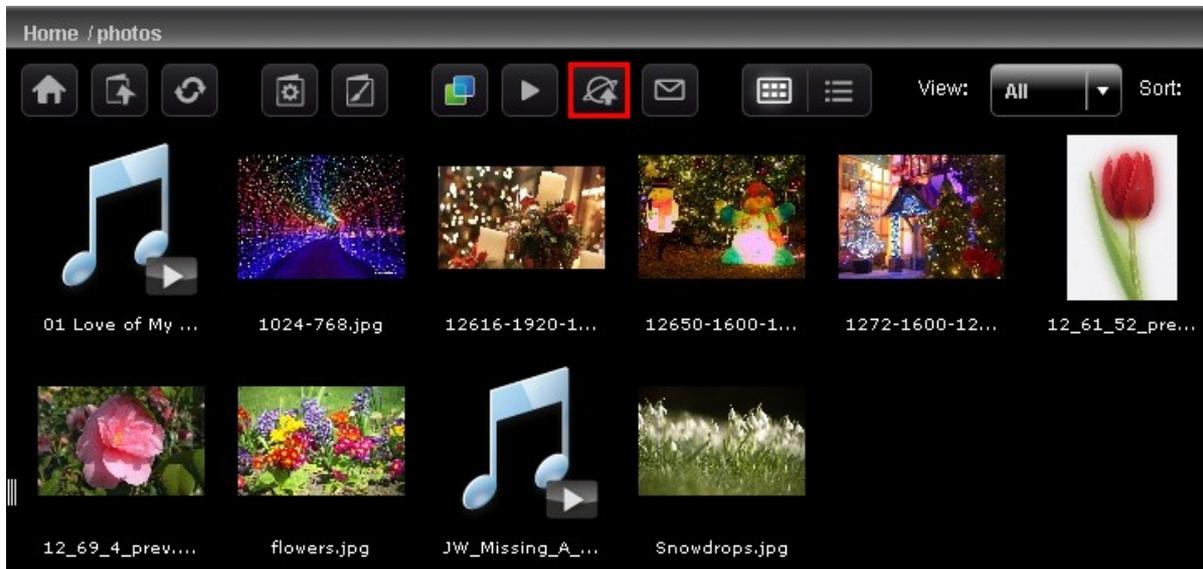
frame for displaying the image file. To view the image files in 3-dimensional (3D) display, click .



Publish image files

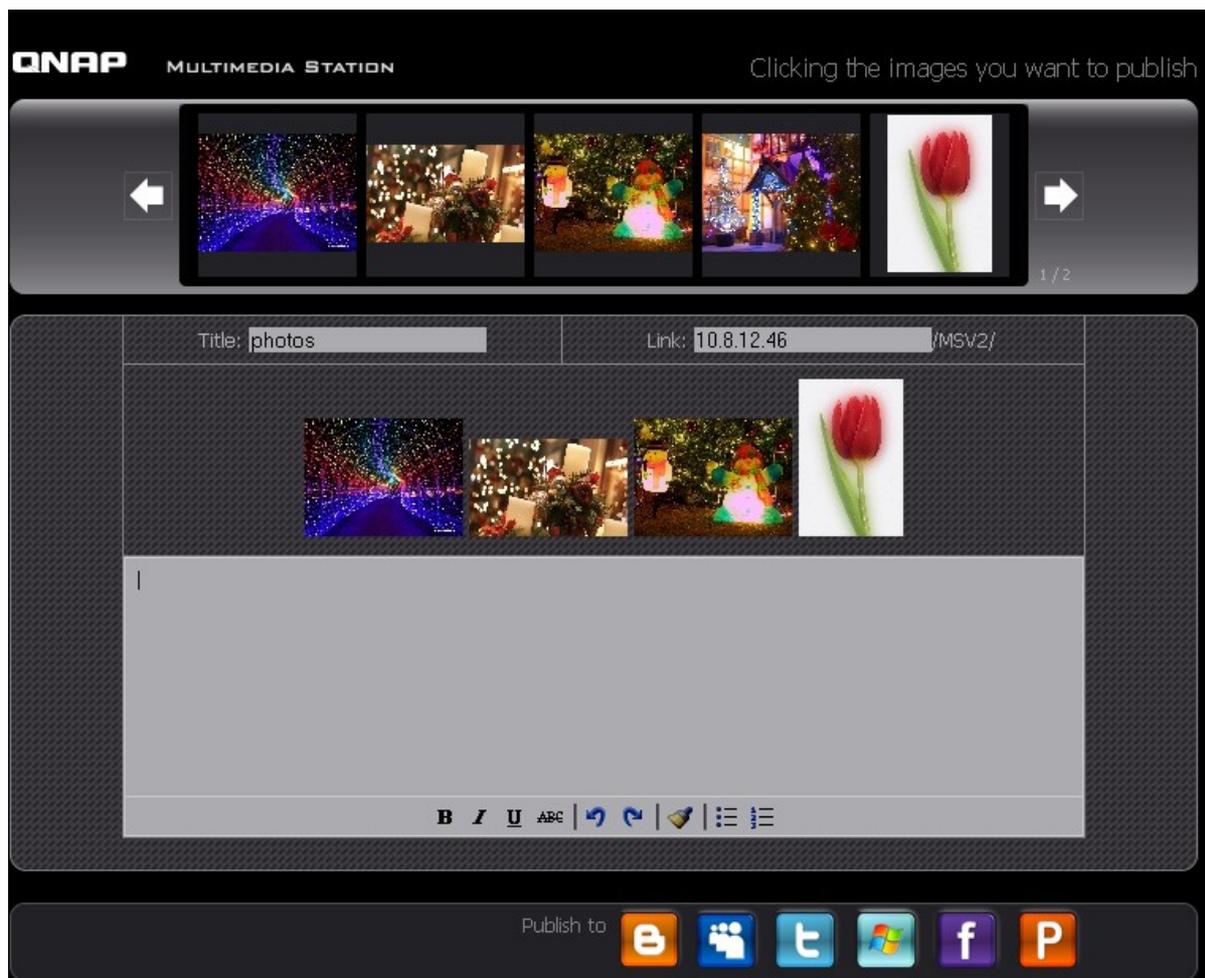
You can publish the image files on the Multimedia Station to social networking sites such as Facebook

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 the 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

QNAP MULTIMEDIA STATION
Clicking the images you want to publish



1 / 2

Selected Images

Subject:

My Name:

My Email:

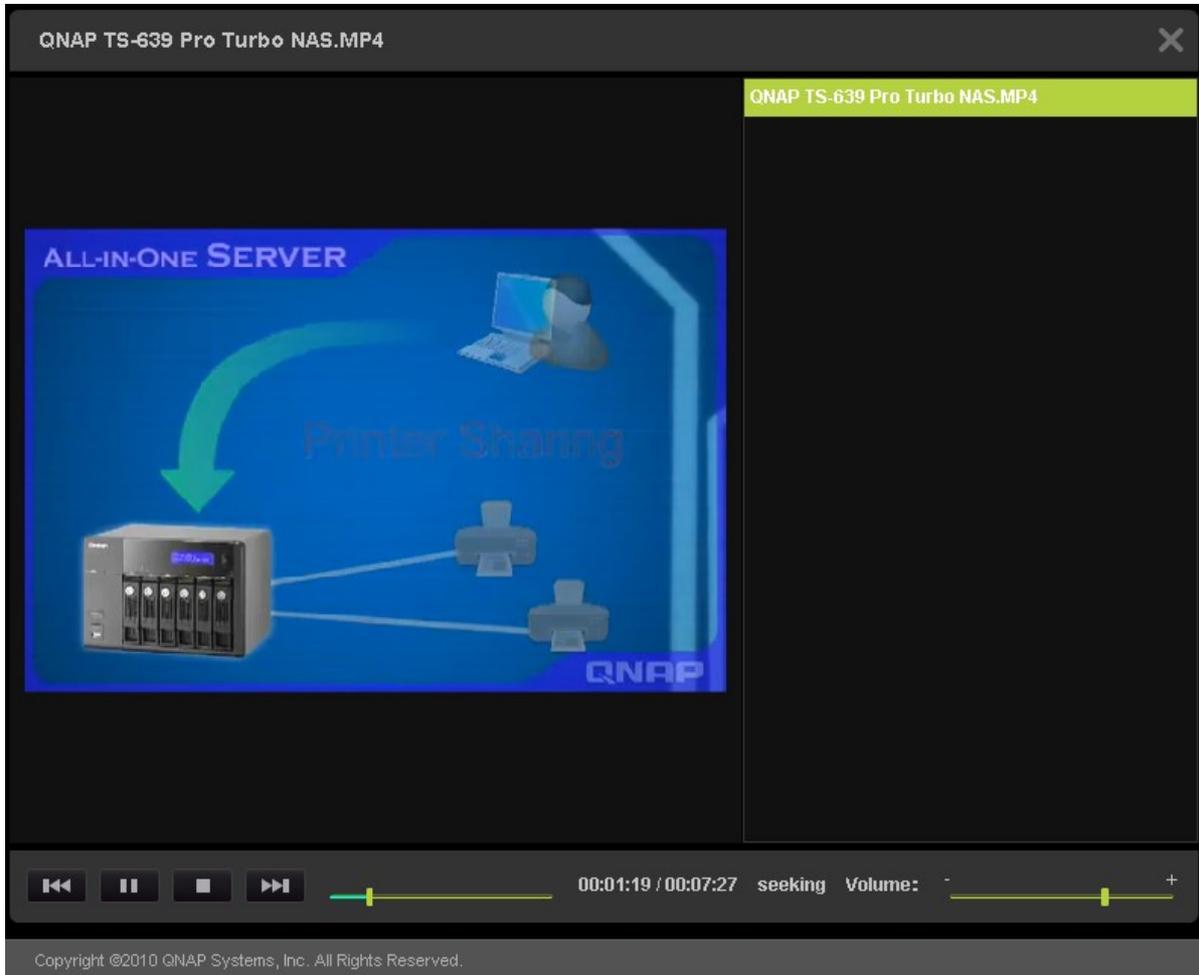
Friend's Name:

Friend's Email:

Message:

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.

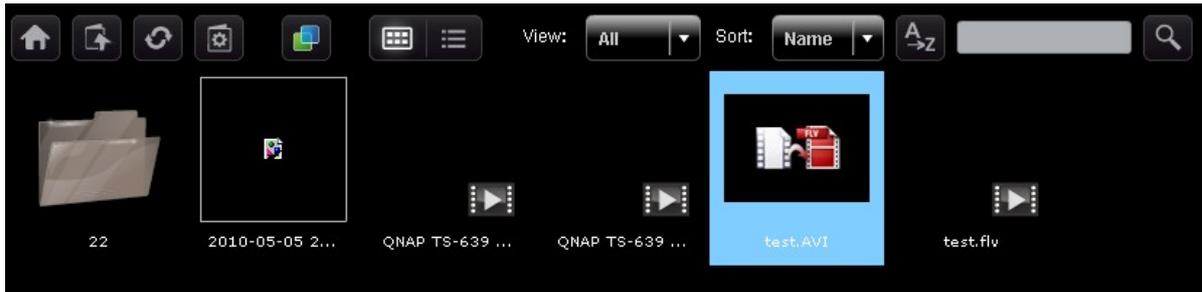


Transcode video

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 the 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 the Multimedia Station supports before uploading the files to the NAS.

Name	Date	Type	Size	
22	2010/05/17	Folder		
2010-05-05 22-00-07~22-01-09.avi	2010/05/17	video	2,010KB	
QNAP TS-639 Pro Turbo NAS.MP4	2010/05/13	video	27,849KB	
QNAP TS-639 Pro Turbo NAS_2.MP4	2010/05/17	video	27,852KB	
test.AVI	2010/05/17	video	129,870KB	
test.flv	2010/05/17	video	40,477KB	

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 the Multimedia Station.

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

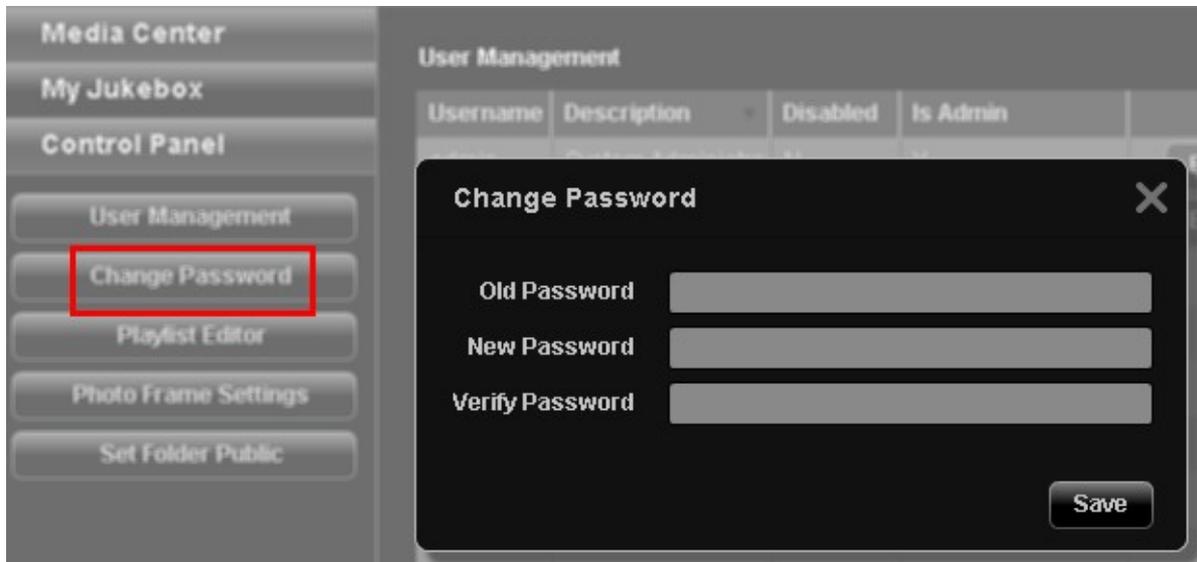
Specify whether or not the user is an administrator and the folders that the user can or cannot access. Click "Save". Note that the password must be 1 to 16 characters long. It can only contain A-Z, a-z, 0-9, -, !, @, #, \$, %, _, .

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.

User Management						
Username	Description	Disabled	Is Admin			
admin	System Administra	N	Y	Edit User		
test		N	N	Edit User	Delete User	Change Password

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 the 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

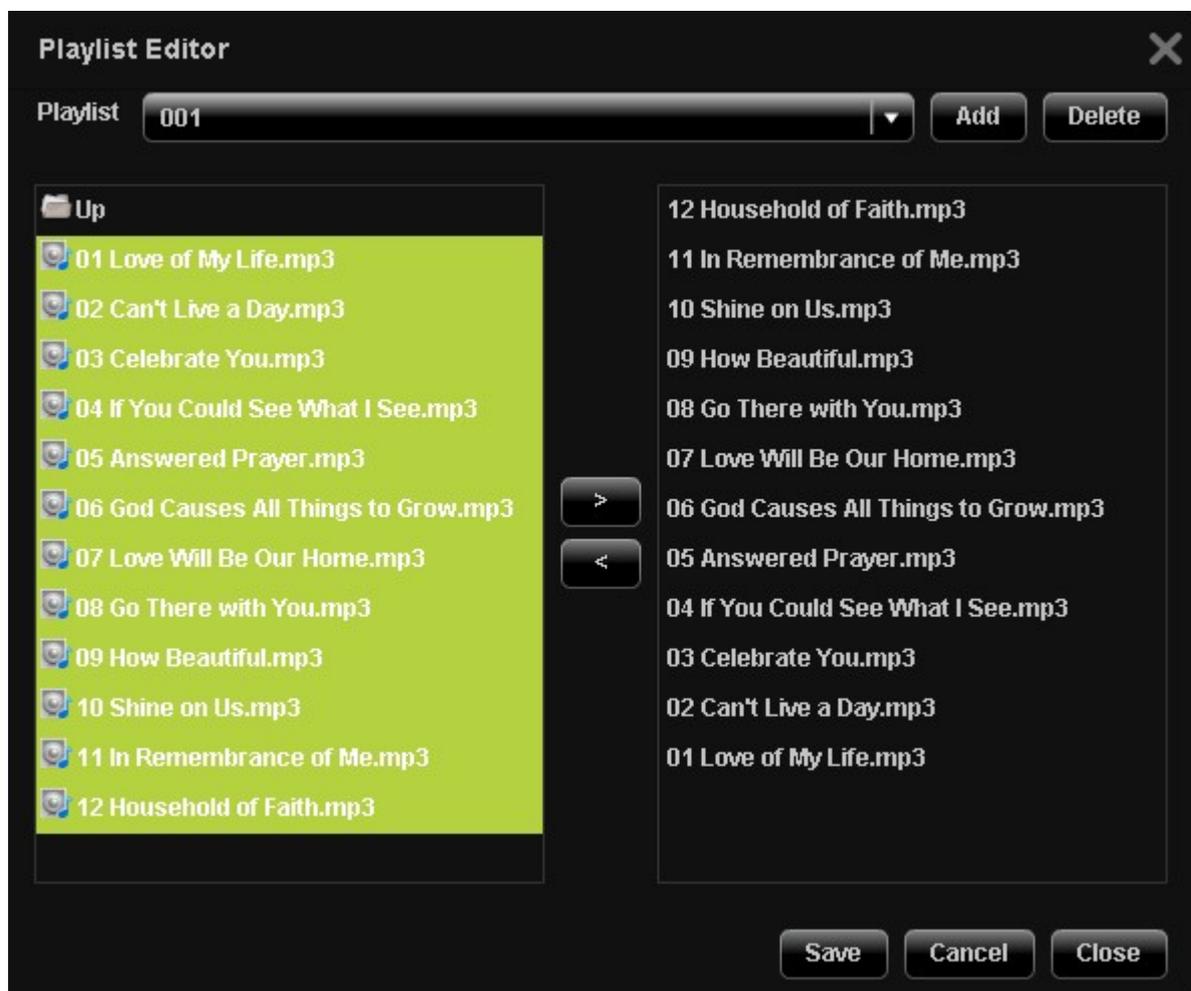
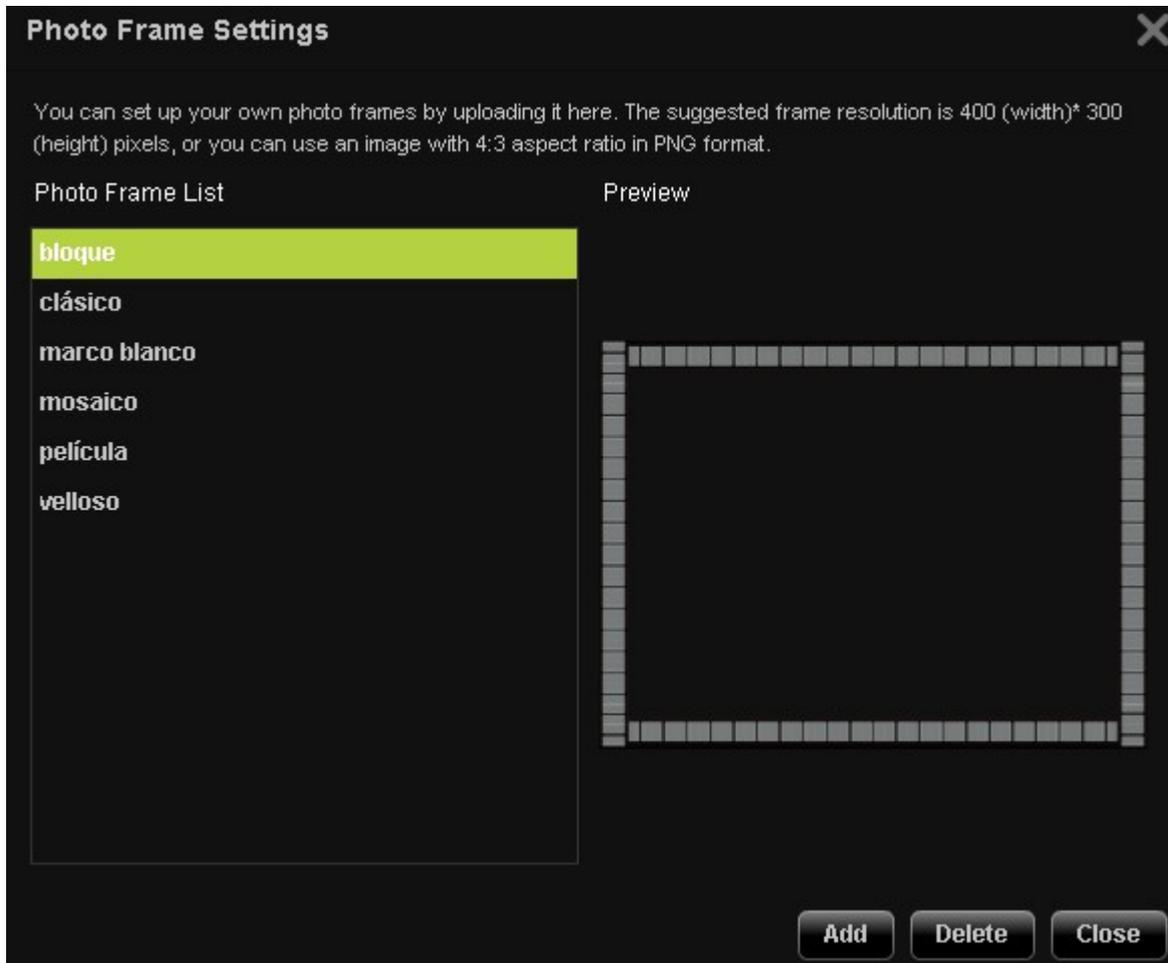
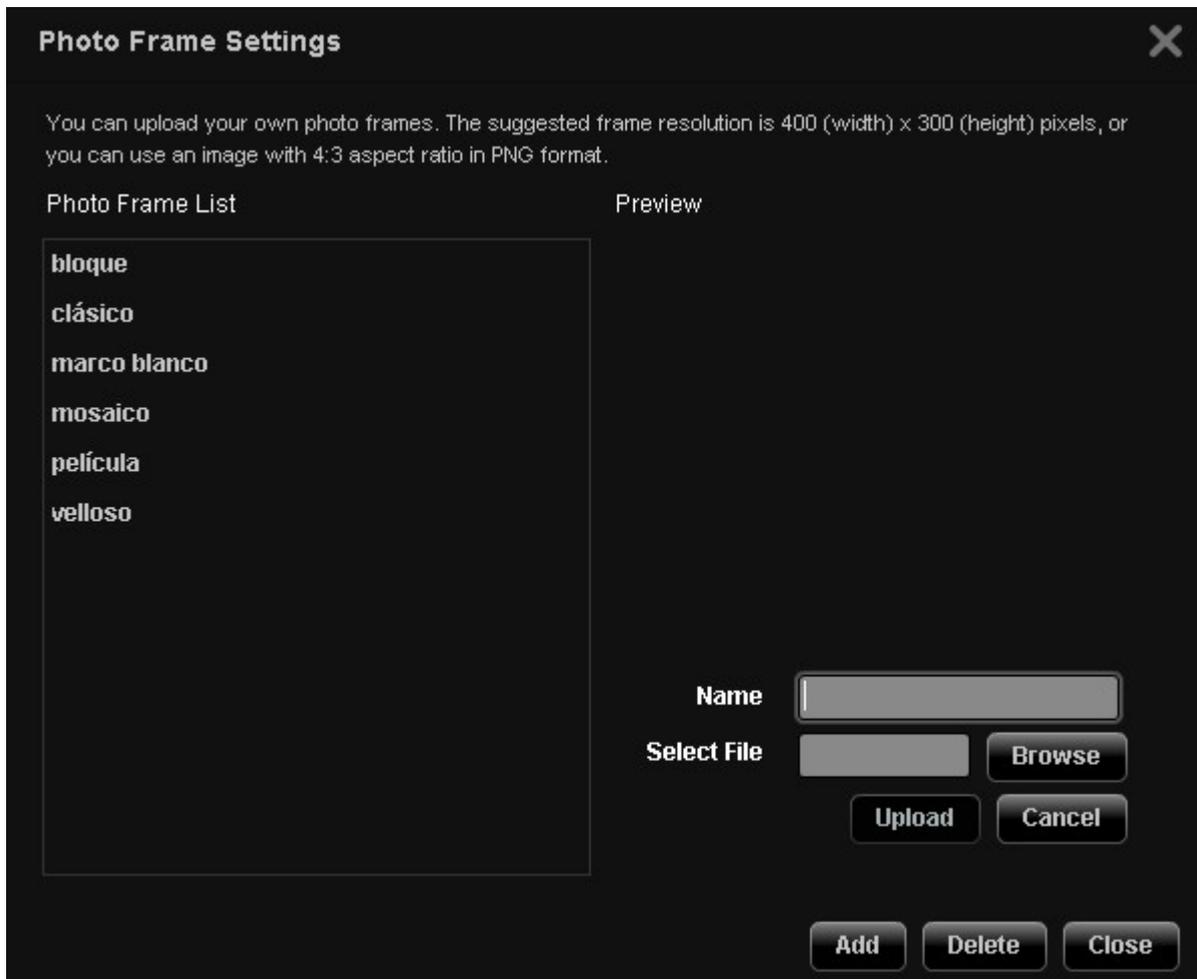


Photo Frame Settings

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.

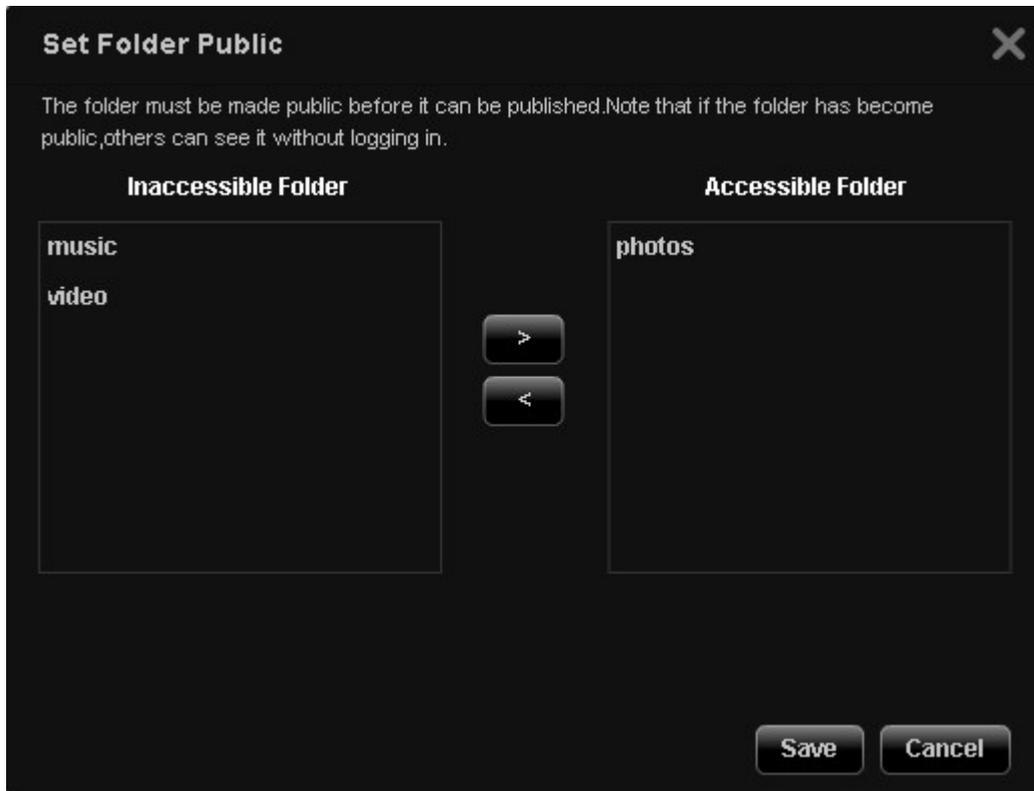


The name of a photo frame must be 1 to 16 characters long. The maximum number of photo frames the Multimedia Station supports is 64 (including the system default photo frames). Note that the system default photo frames cannot be deleted.



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 the 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/>

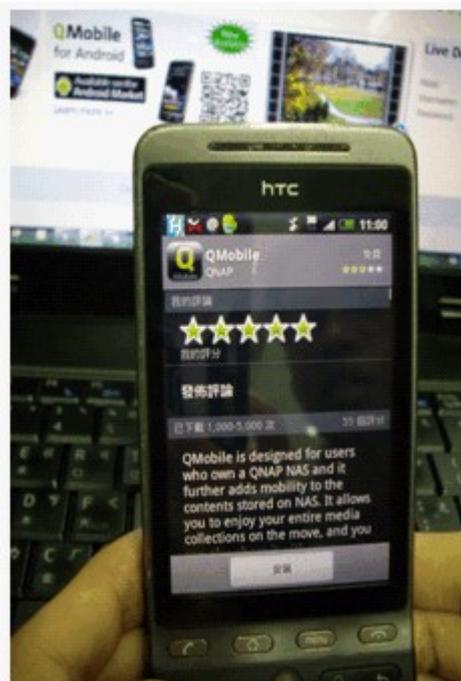
Take a picture of the QR-code.



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, iPad, iPod touch" on the NAS under "Network Services" > "Network Service Discovery" > "Bonjour".

Home >> Network Services >> Network Service Discovery

Service Name: nas(AFP)

SSH
Service Name: nas(SSH)

FTP (File Transfer Protocol)
Service Name: nas(FTP)

HTTPS (Secure web server)
Service Name: nas(HTTPS)

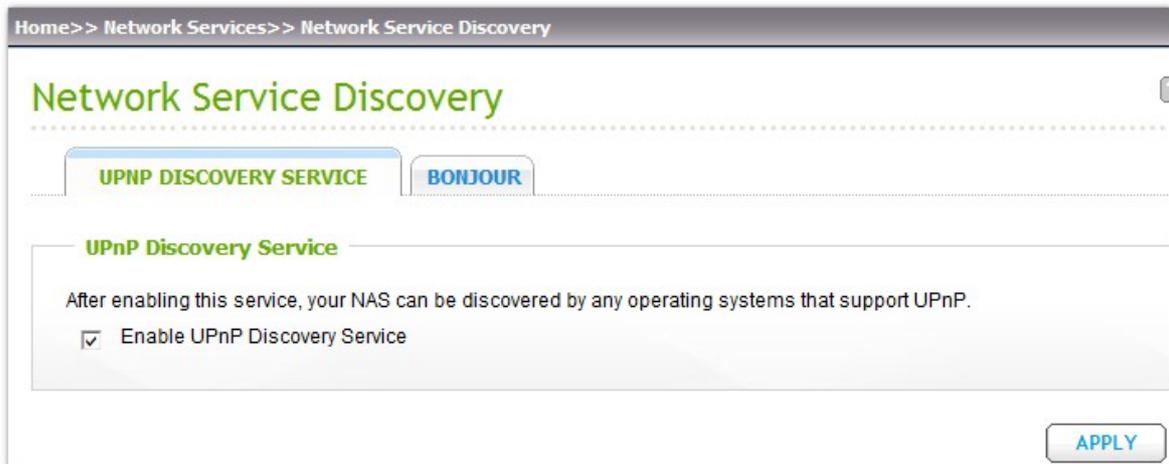
DLNA Media Server
Service Name: nas(DLNA)

Apps for iPhone, iPad, iPod touch
Service Name: A-439(QMobile)

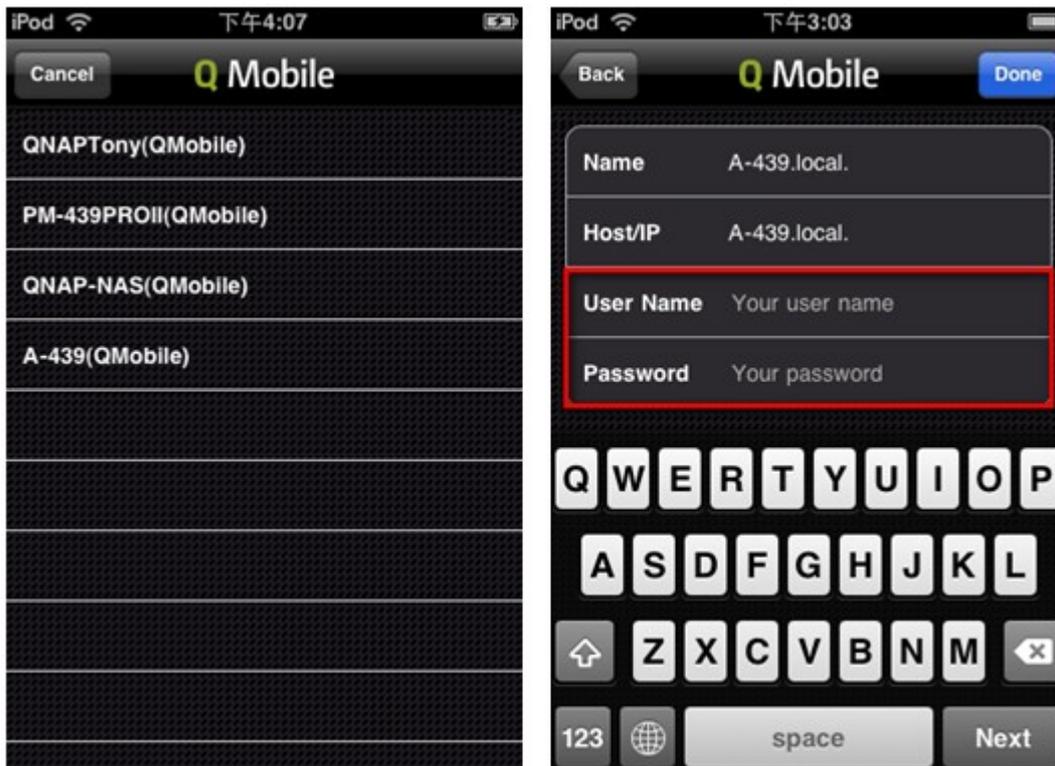
APPLY

2. For Android devices

This feature is only available after you have enabled "Enable UPnP Discovery 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 username and password.



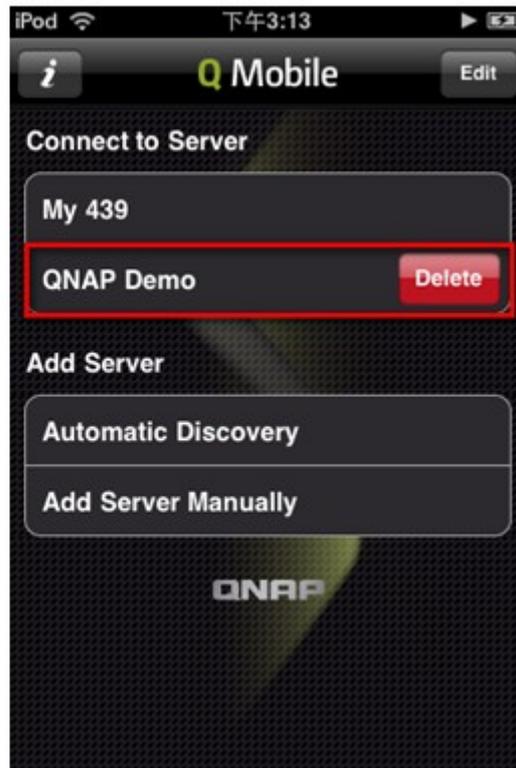
Add Server Manually



Enter the name, host/IP, username 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.

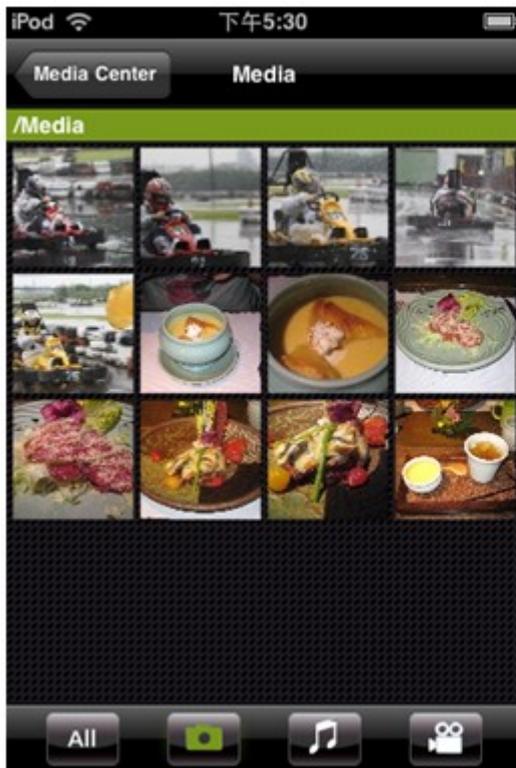
Connect to the NAS and tap the Media Center icon.



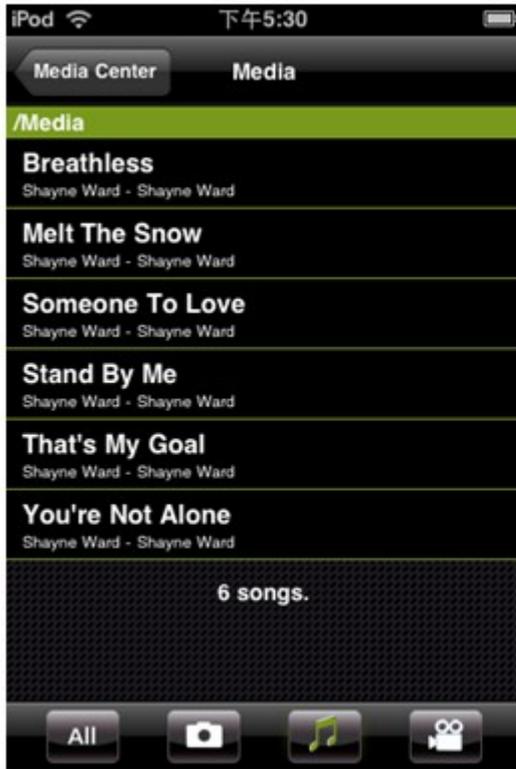
You can browse the multimedia files under "Qmultimedia/Multimedia" default network share or you may choose the specific photo, music or video files by tapping the corresponding icon at the bottom.



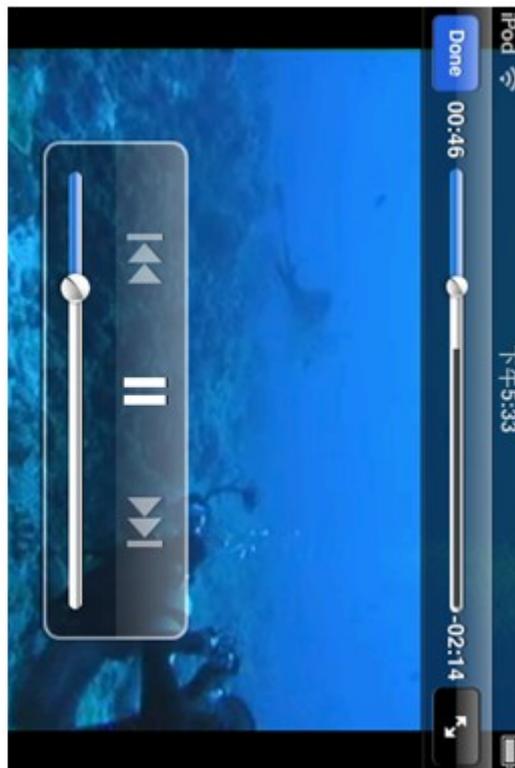
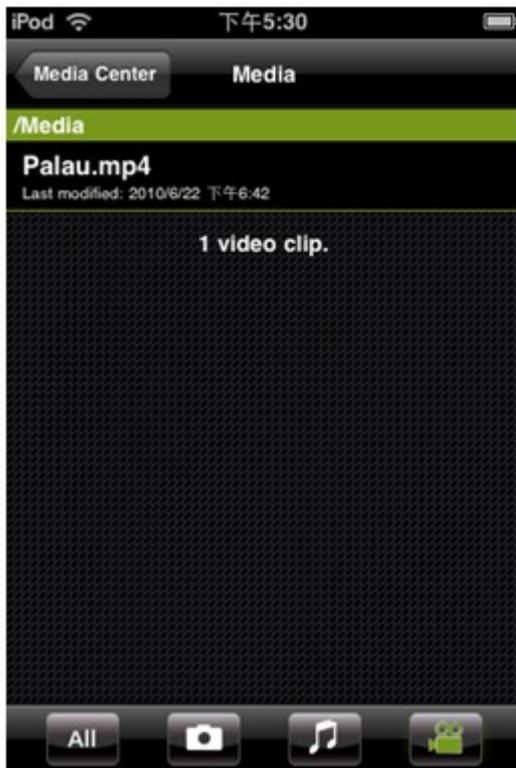
Photo view



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 .

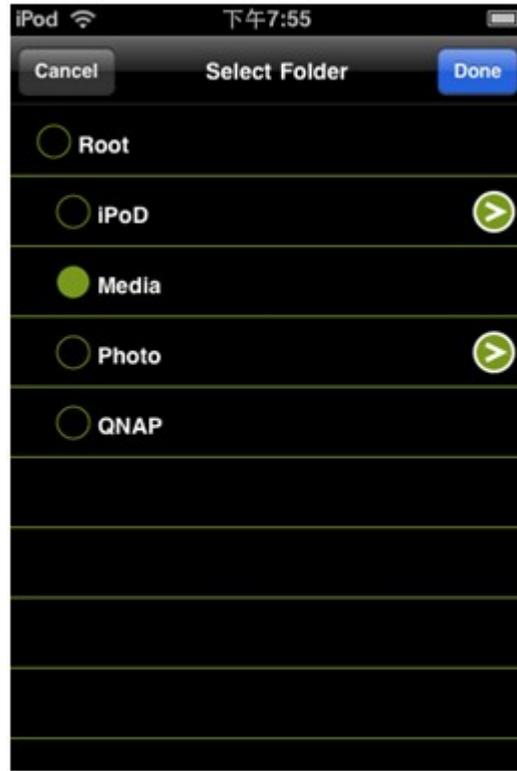


Photo Source: Choose the photos from your handheld devices.

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

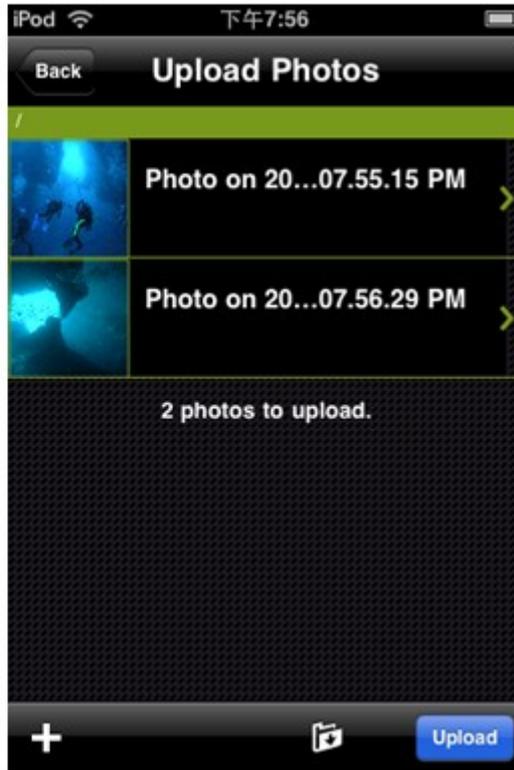


(Photo source)



(Photo destination)

Select the photos and tap the "Upload" icon to upload the photos to the NAS.

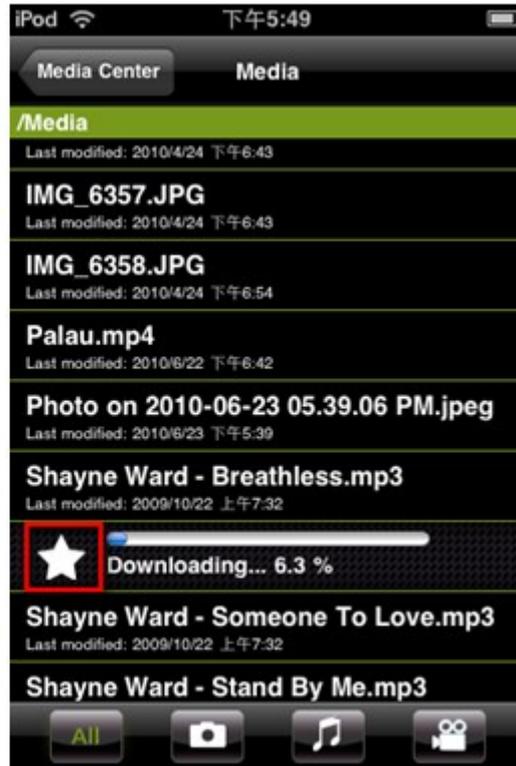


3. My Favorites

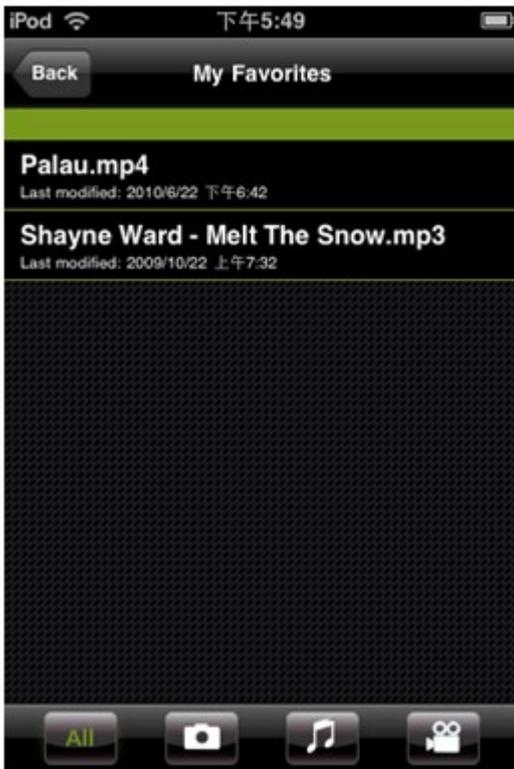
You may download the multimedia files from the NAS to your handheld devices under "My Favorites" and play them offline.



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".)



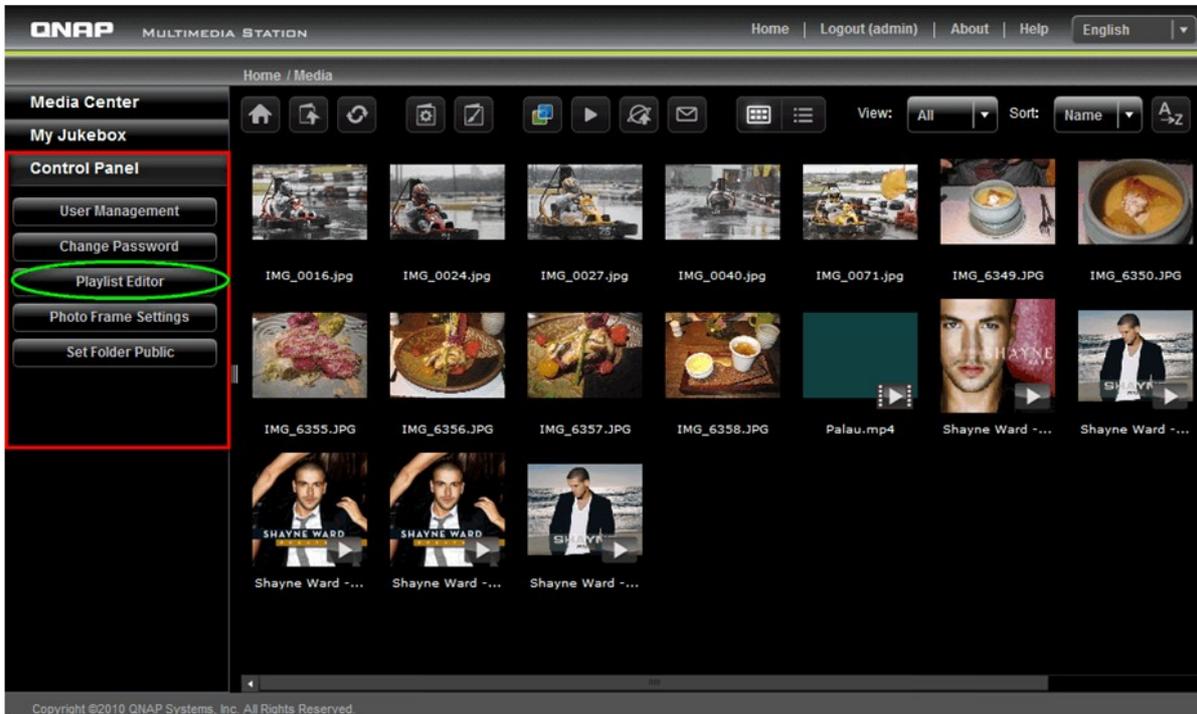
Downloaded files will be shown in "My Favorites". QMobile will check if the source of the downloaded files have been updated or deleted from the NAS upon every new connection to the NAS. You can select to synchronize the changes with the NAS.



4. My Jukebox

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

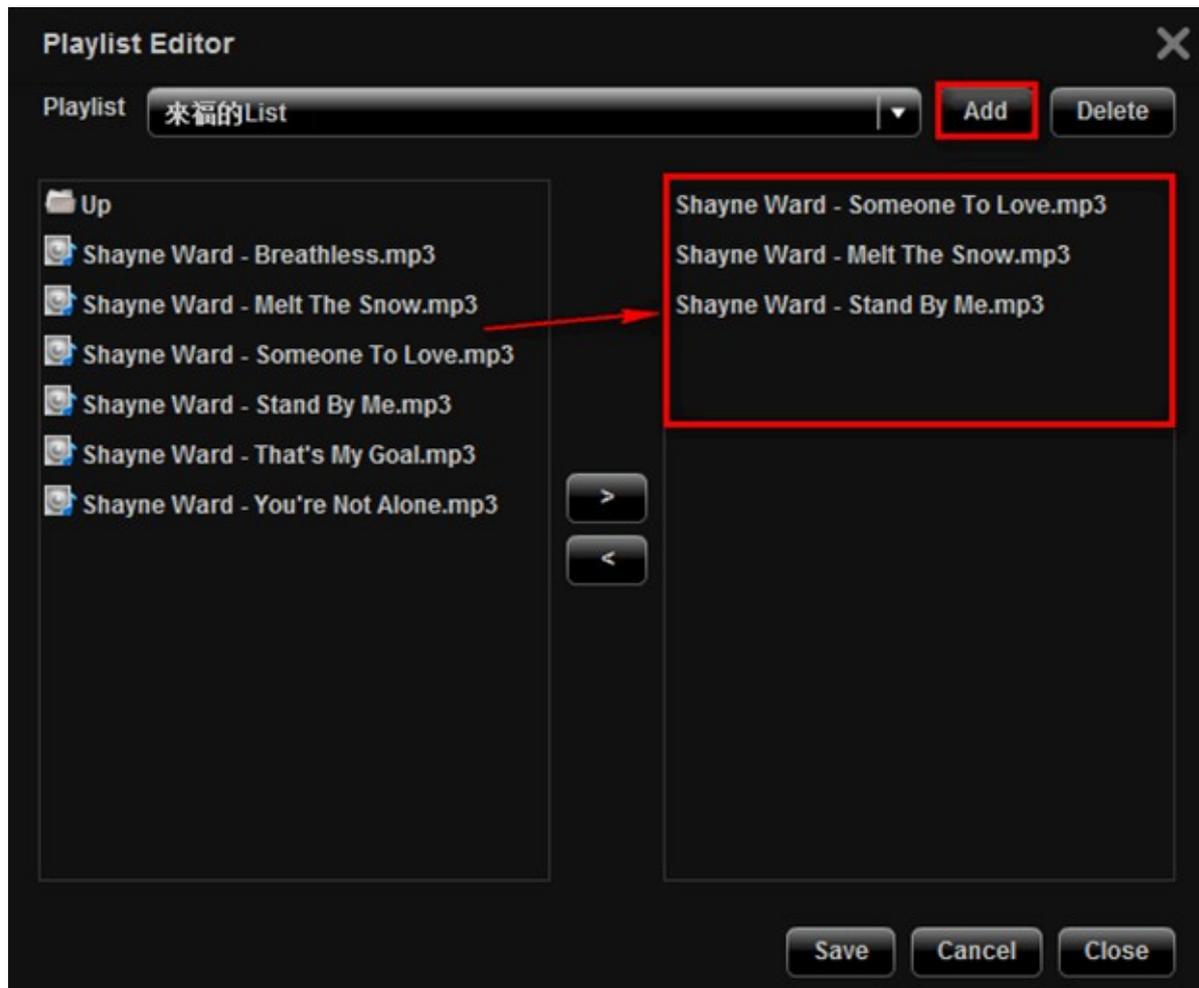
Login Multimedia Station as an administrator. Select "Control Panel" > "Playlist Editor".



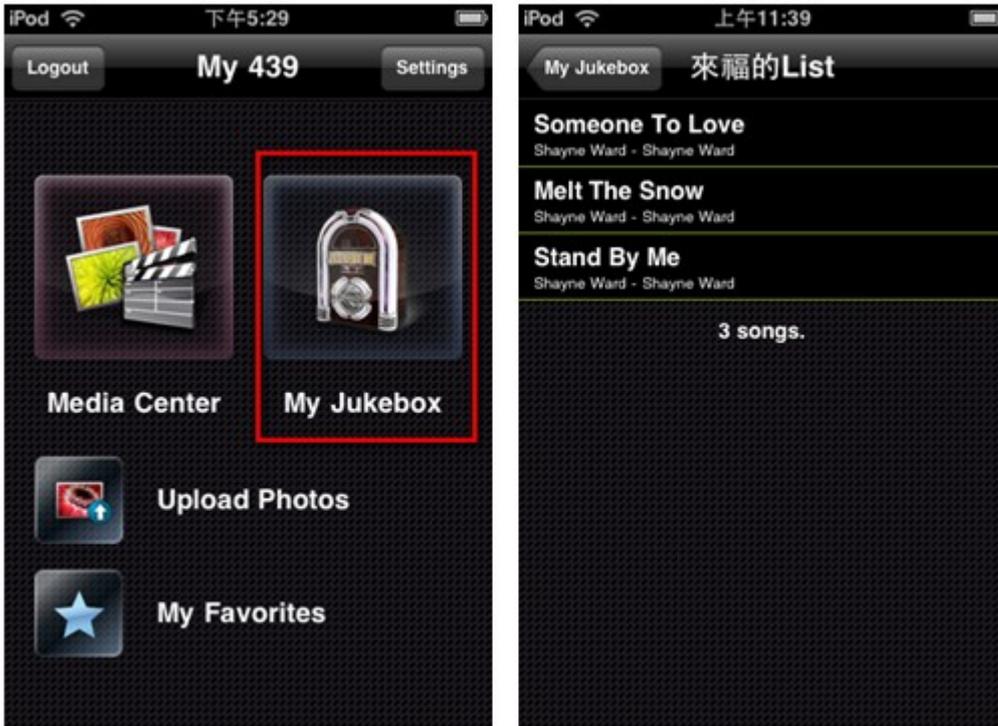
Click "Add" to create a Playlist. Enter the playlist name and click "Save".



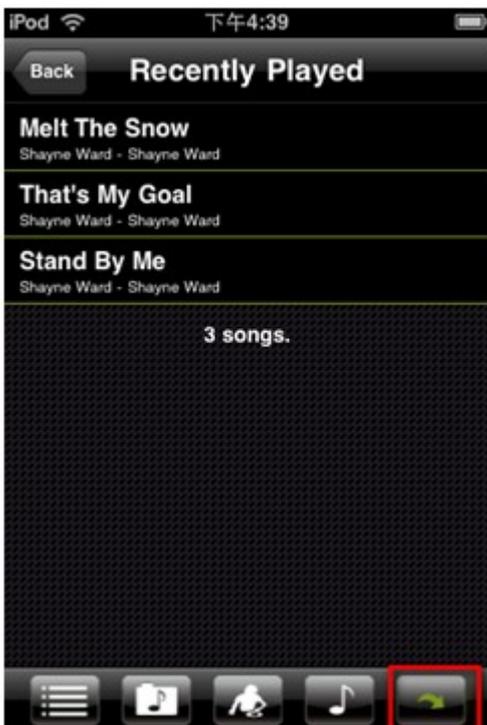
Select the playlist from the drop-down menu and then choose the music files to add to the playlist and click ">". Click "Save" to save the playlist.



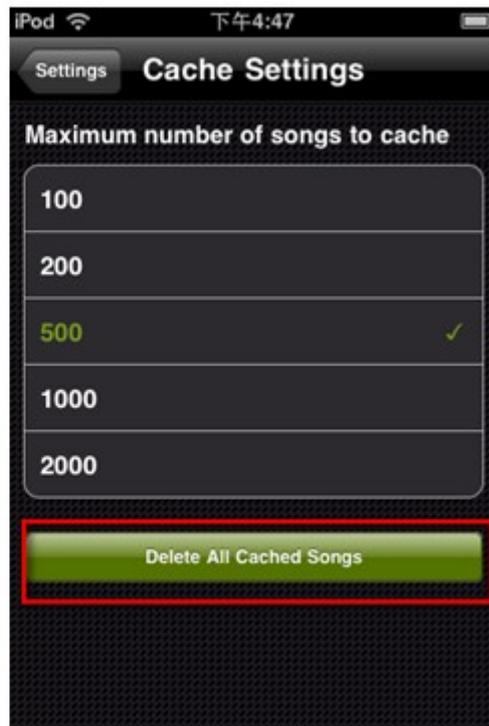
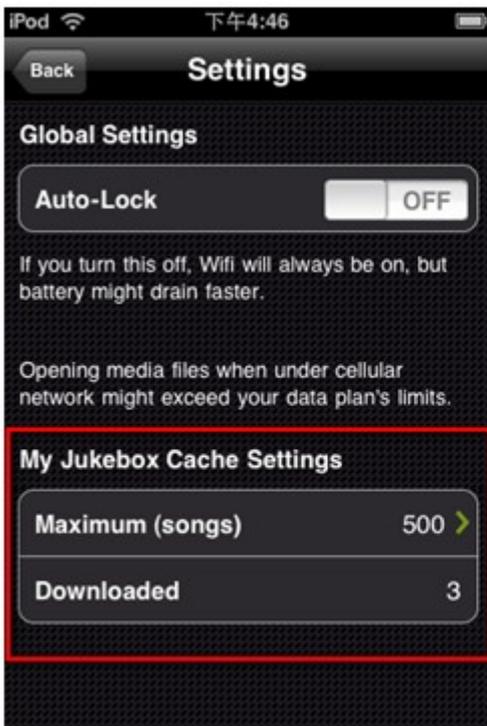
You can play the playlists created on the NAS by "My Jukebox" on your handheld devices.



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

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

Requirements:

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

To use the Photo Station, do the following.

1. Login the NAS as "admin". Go to "Administration" > "Applications" > "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.

Photo Station

Photo Station

Enable Photo Station

After enabling this service, you may click one of the following links to enter Photo Station.

<http://10.8.13.59:80/photostation/>

<https://10.8.13.59:8081/photostation/>

Rescan media library

Daily start time: 00 : 00

The administrator accounts (admin) for local NAS administration and the application are the same. Please login as "admin".

Select either "System Users" or "Standalone Application Users" as the user accounts for the application. If "System User" is selected, set up the users and the access rights in "Access Right Management" > "Users". Otherwise, go to the application's page to set up the user accounts.

User Account Settings: Standalone Application Users

APPLY

2. Select either "System Users" or "Standalone Application Users" (default) for the user account settings. When "System Users" is selected, the local NAS accounts will be used for the application. You can create the user accounts in "Access Right Management" > "Users". To use dedicated user accounts for the application, select "Standalone Application Users". The user accounts can be created and managed after logging in the application under "Settings".

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

The Photo Station supports the following file format:

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

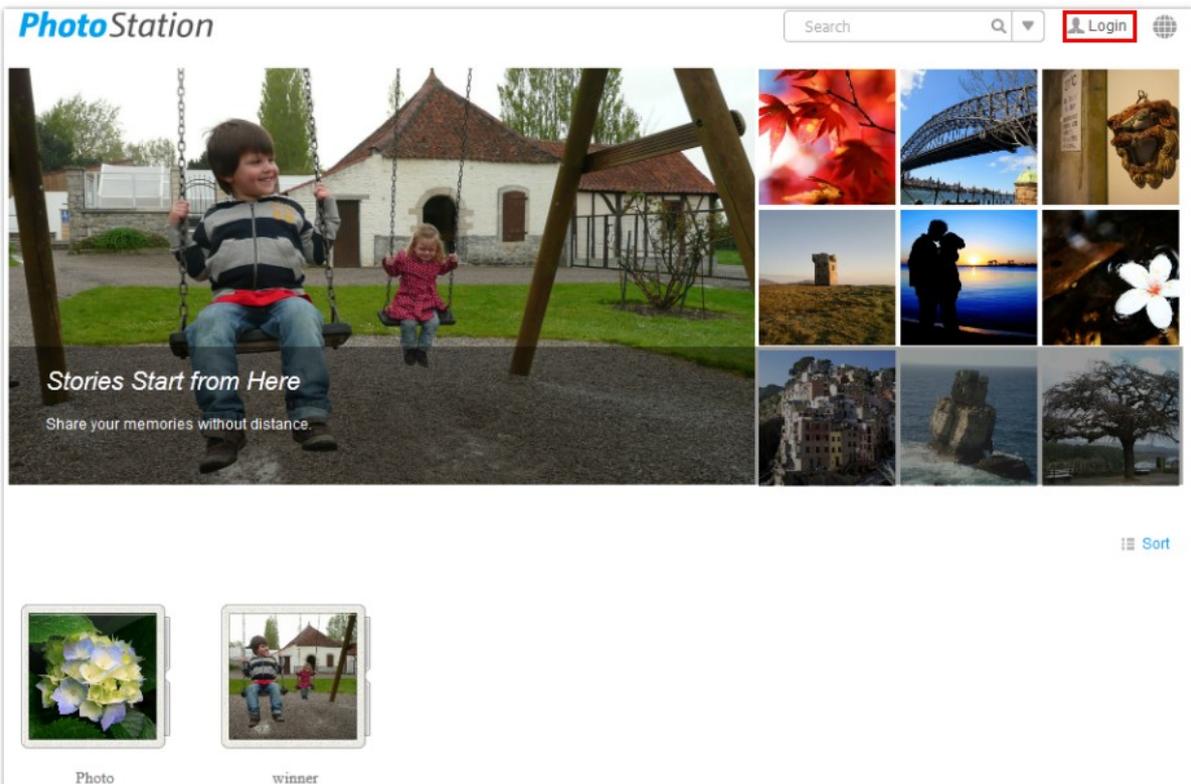
Tips on file upload:

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

4. Connect to the Photo Station from the login portal of the NAS or enter <http://NAS IP/photostation> in a web browser (Internet Explorer, Mozilla Firefox, or Google Chrome) and click "Login" to login the Photo Station.

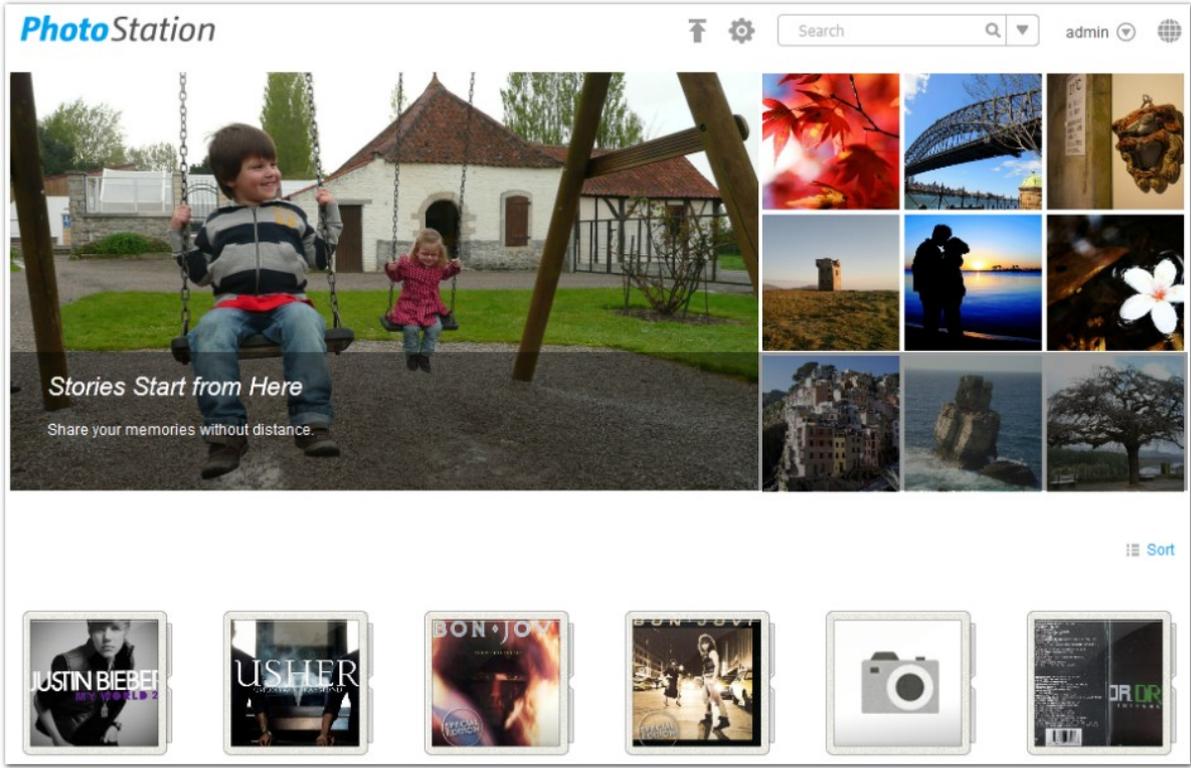
Note:

- The admin login information of the Photo Station is the same as that of the NAS web administration.
- Login to the application from the login portal of the NAS will be disabled when standalone user accounts are in use, except for "admin".



5. The banner and description of the Photo Station are shown on the upper section of the login page.

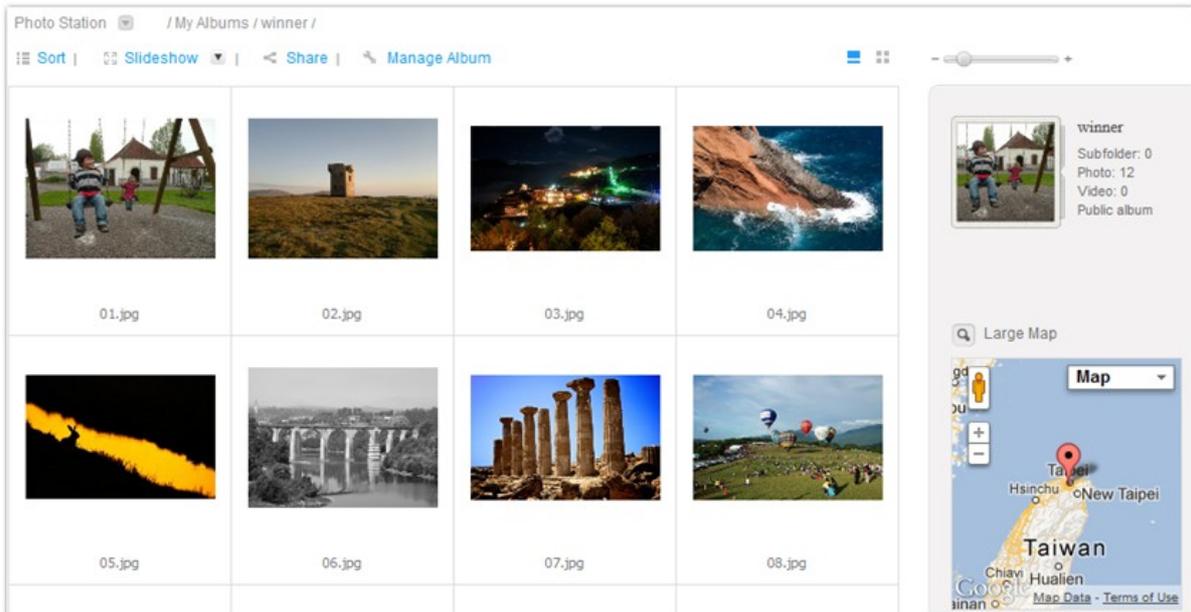
Below the banner are the albums accessible by the user account. Click  to select the display language.



Icon	Description
	Upload photos and create an album or add photos to an existing album.
	Go to the Settings page.
	Search for the folders, photos, or videos under the current directory. Click the triangle icon for advanced search.
	Logout; about the Photo Station.
	Select the display language.
	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)

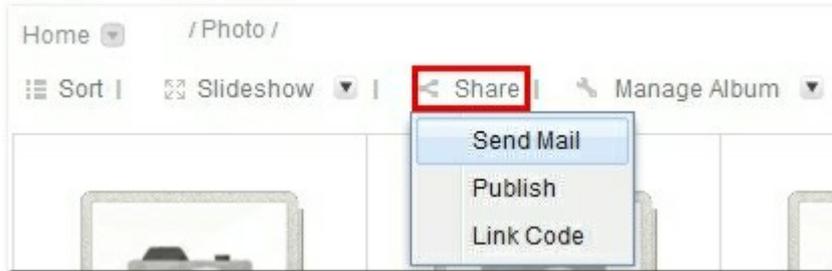
When browsing an album (a folder), the subfolders and supported images and video files will be shown.



Icon/Option	Description
	Navigate to the parent folders.
/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 the Music Station ("Applications" > 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.
	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.
	Adjust the thumbnail size.

2. Share photos and video files

The images on the 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.



Click the images you want to publish

Selected Images

Subject:

My Name:

My Email:

Friend's Email:

Message:

You can post your personal message here.

Note: Separate the email addresses by comma (,) or a semi-colon (;).

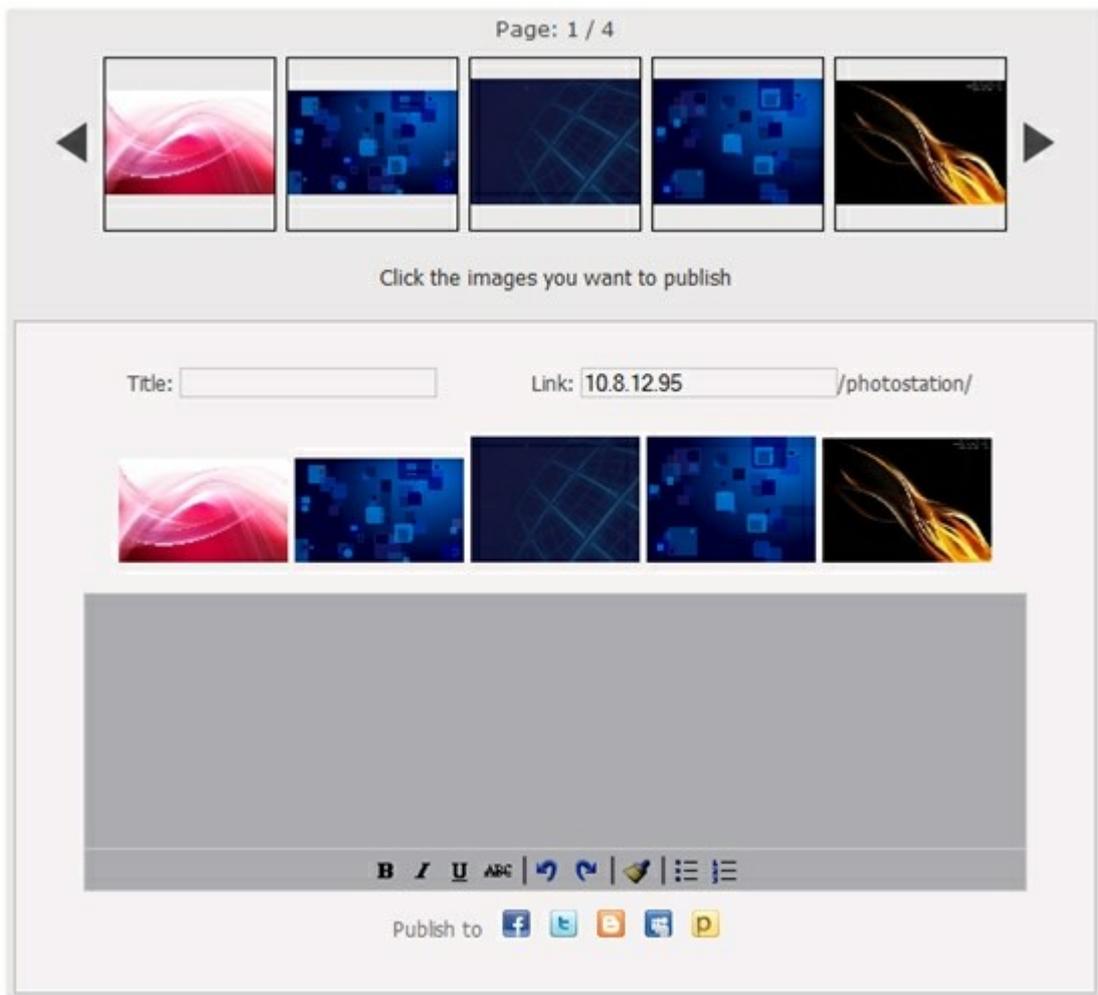
Attach slideshow link

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.
- The 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.



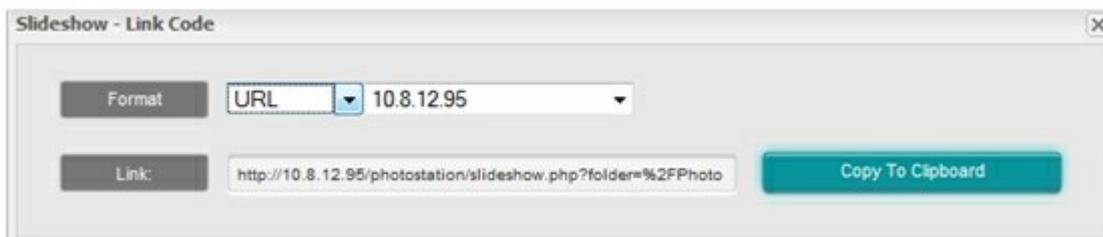
The screenshot shows the 'Publish' interface of the Photo Station. At the top, it displays 'Page: 1 / 4'. Below this is a horizontal row of five image thumbnails, each with a small white box at the bottom for selection. Navigation arrows are on either side. Below the thumbnails is the instruction 'Click the images you want to publish'. The main area contains a 'Title:' text box, a 'Link:' text box with the value '10.8.12.95 /photostation/', and a row of five smaller image thumbnails. Below these is a large grey text area for a message. At the bottom, there is a rich text editor toolbar with icons for bold, italic, underline, text color, link, unlink, list, and image. Below the toolbar are social media icons for Facebook, Twitter, MySpace, Plurk, and Blogger, with the text 'Publish to' to their left.

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.
- The Photo Station must be accessible on the Internet. It is suggested to set up the DDNS or MyCloudNAS service on the NAS.



Slideshow - Link Code

Format: URL 10.8.12.95

Link: http://10.8.12.95/photostation/slideshow.php?folder=%2FPhoto

Copy To Clipboard

Share Private Albums

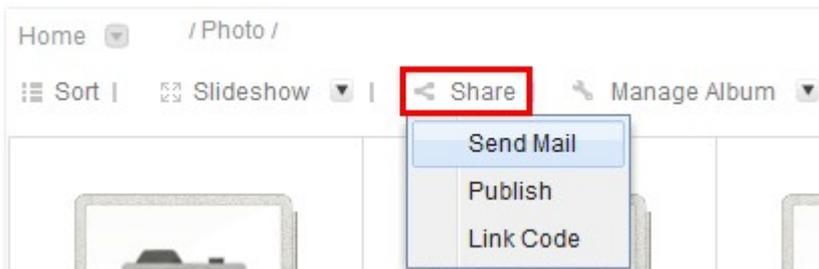
Click "Manage Album" and select "Enable/Disable Slideshow Link".



Enable slideshow link and enter an access password for the slideshow link.



Click "Share" to share the album by email or link code.

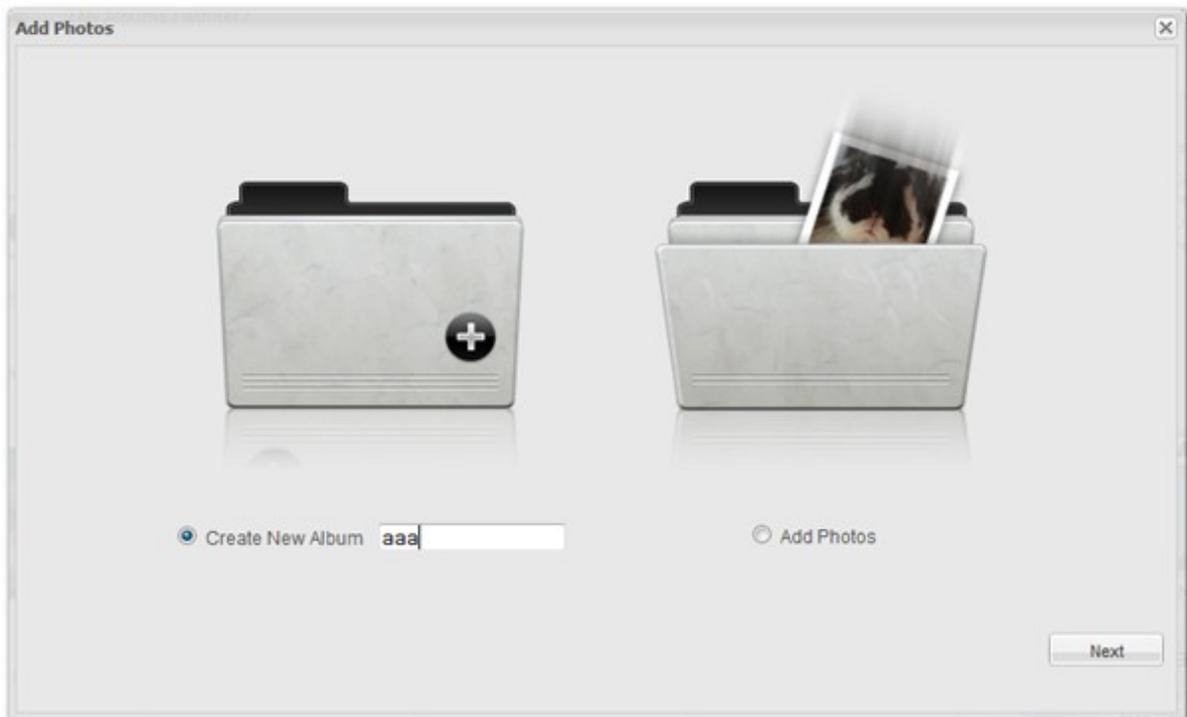


3. Create an album

To create an album in a folder, click "Manage Album" > "Add Photos" or click  .



Select "Create an Album" and enter the album name. Click "Next".

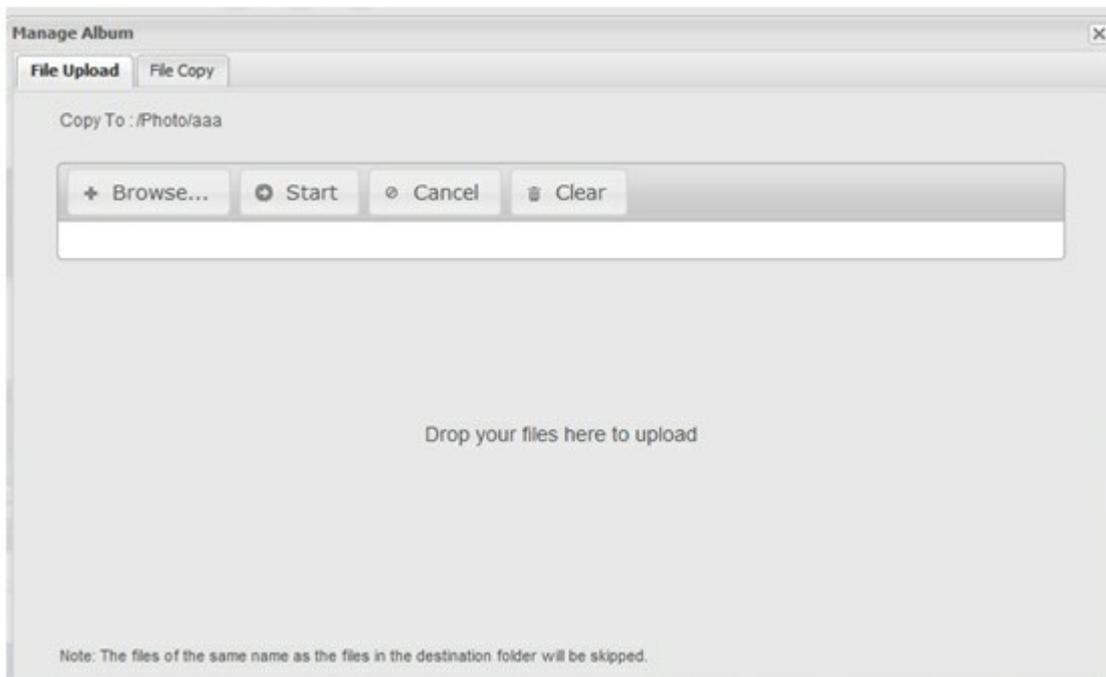


3.1 File upload

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.

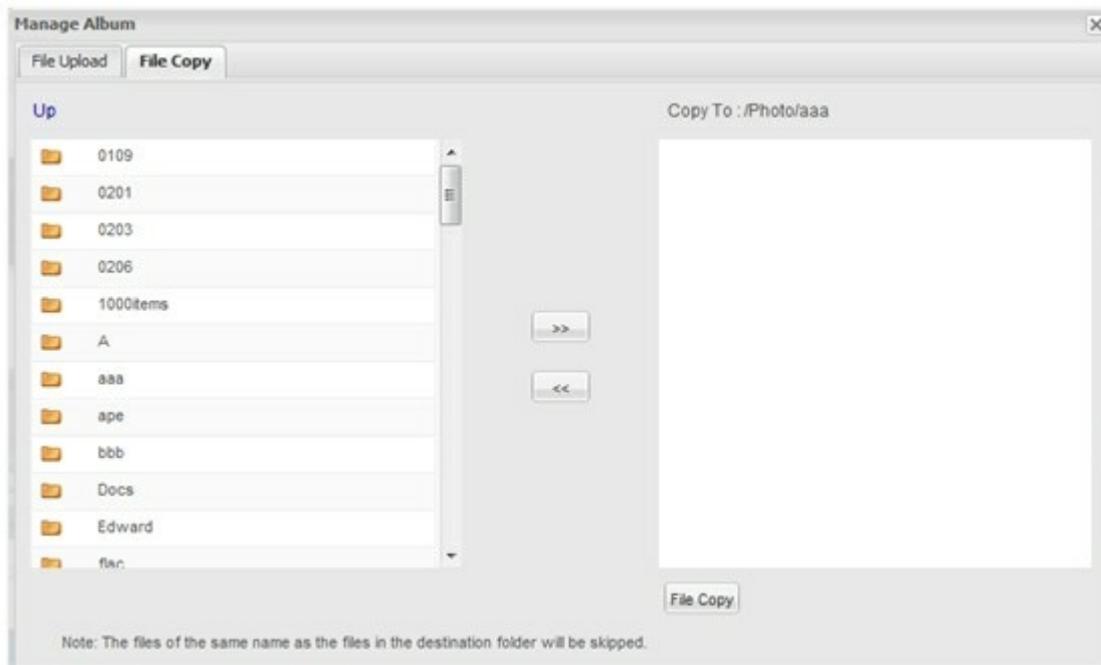
Note:

- 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 the 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.



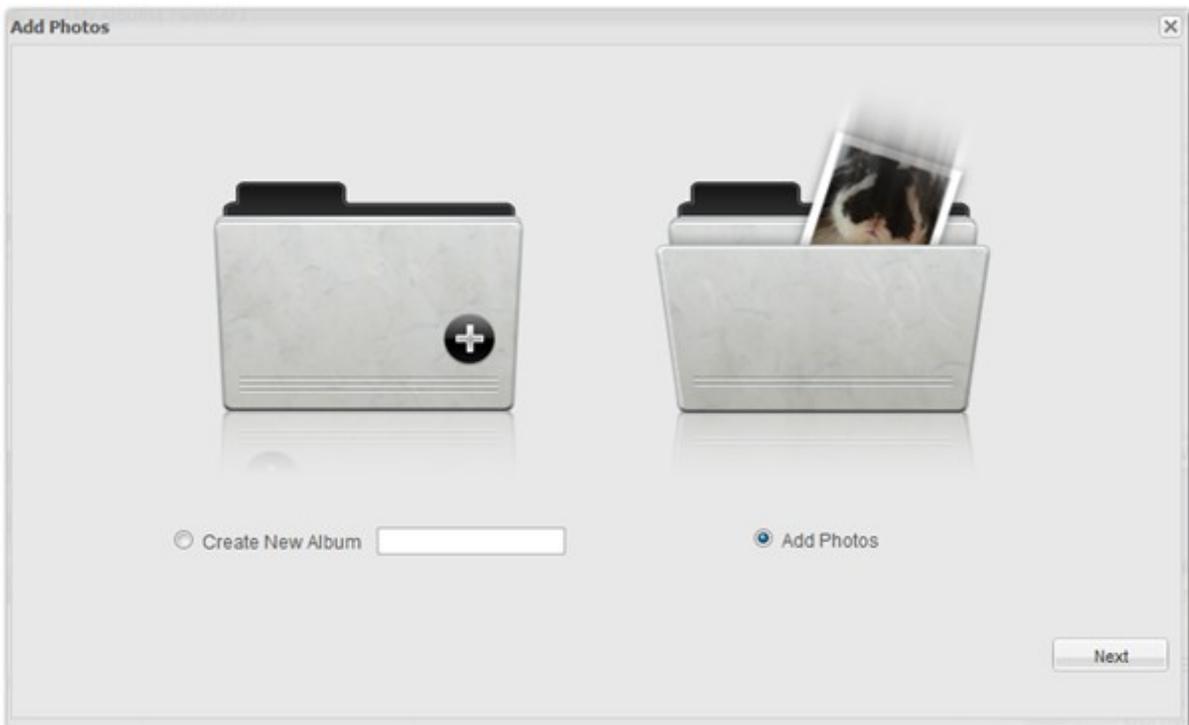
4. Edit an album

To upload or copy files to an existing album on the Photo Station, click "Manage Album" > "Add Photos"

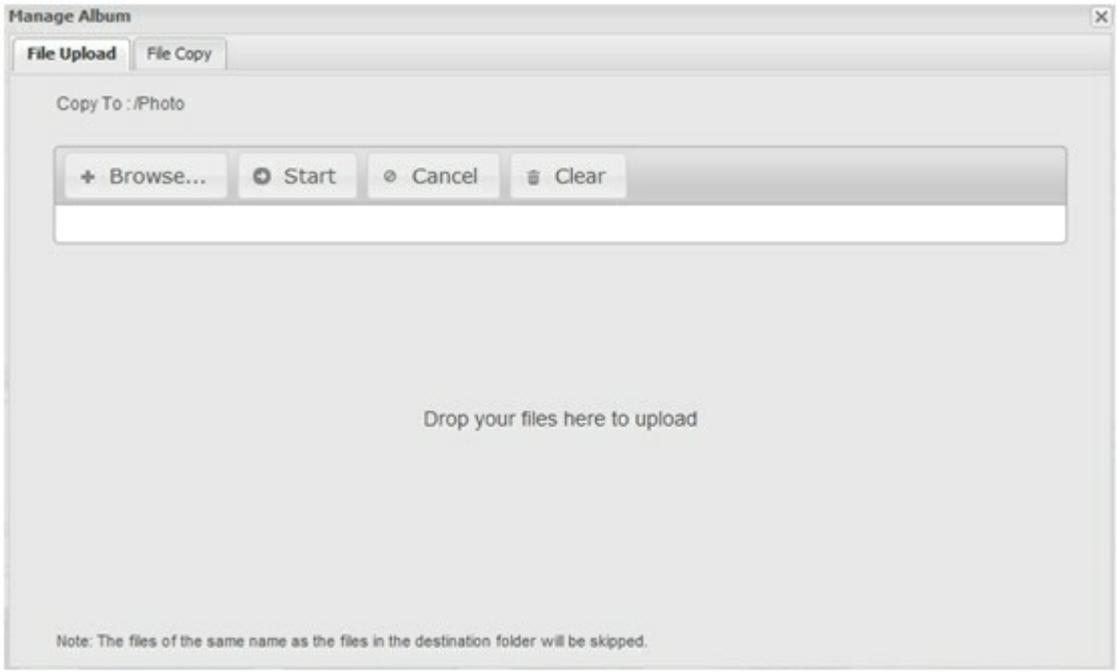
or click .



Select "Add Photos". Click "Next".



Select to upload files or copy files from existing albums to the album.

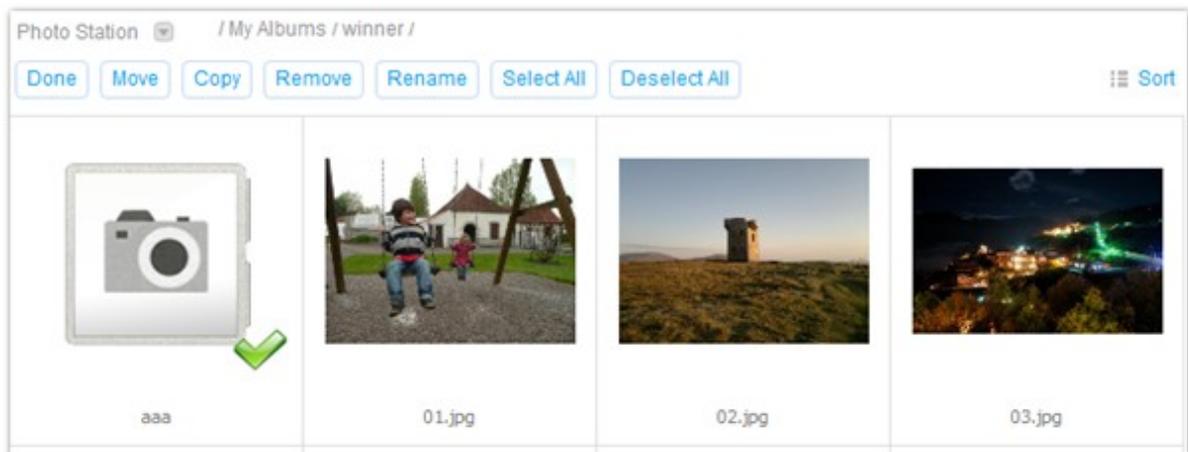


Organize photos

To organize the photos in an album, click "Manage Album" > "Organize Photos".



Choose to move, copy, remove, or rename the files or folders in an album. Click "Done" when the changes are finished.



5. View a photo

The Photo Station supports the following options for viewing an image file.

Icon/Option	Description
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 ("Applications" > Music Station").
Download	Download an image.
Link Code	Copy the links of an image in different sizes for publishing on the Internet.
EXIF	View the EXIF information of an image.
Edit (Pixlr Editor)	Edit the image online by Pixlr Editor.
Geotag	Geotag the image with Google Maps.
	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.

Photo Station / My Albums / winner /

Slideshow | Download | Link Code | EXIF | Edit (Pixlr Editor) | Geotag



01.jpg
Click here to edit the description

Add Comment ▾

admin

Comment

Submit

Comment ▾

1 / 12



Large Map

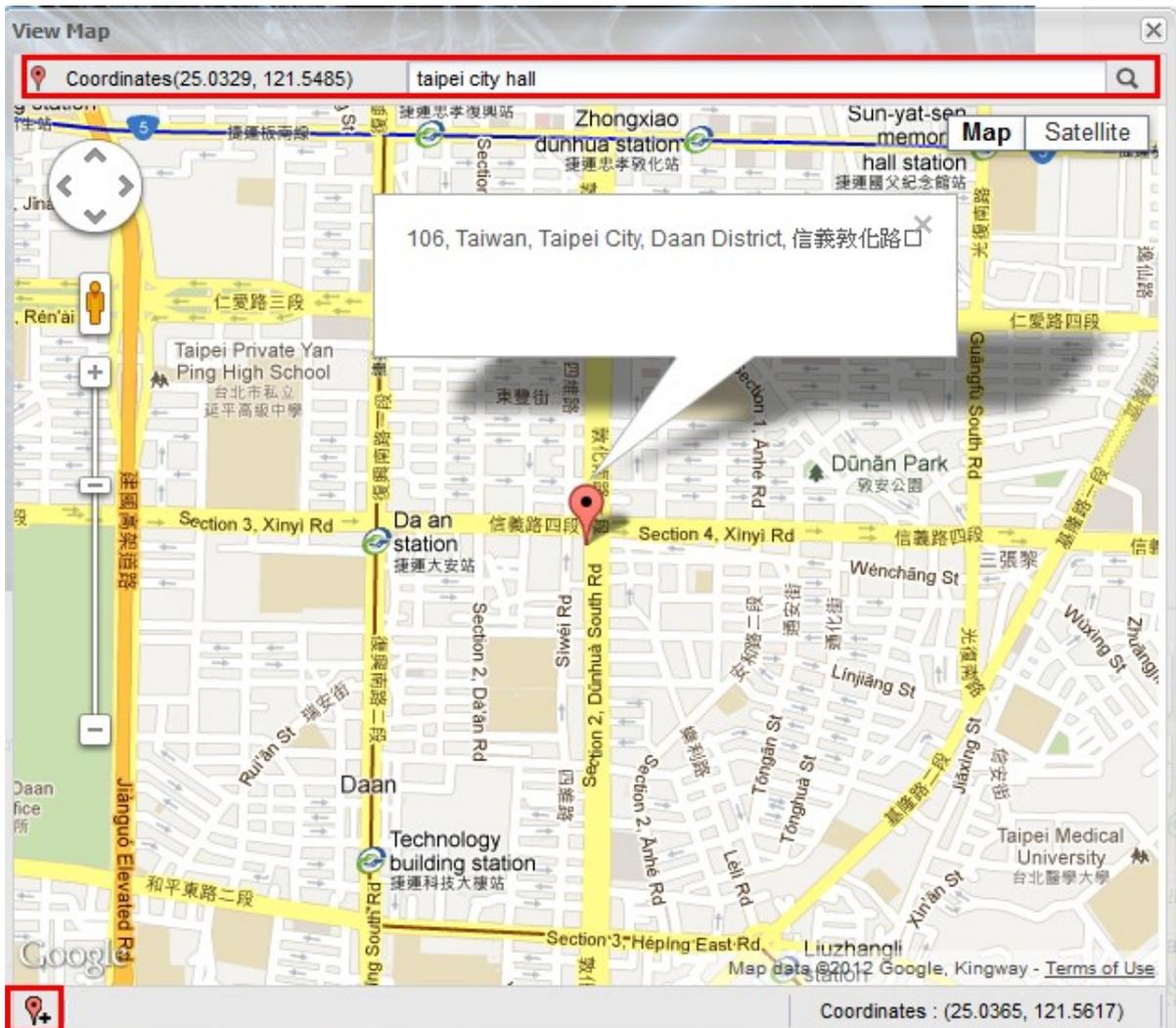
Geotag this photo



Geotag photos



To geotag a photo with Google Maps, click "Geotag" or . 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.



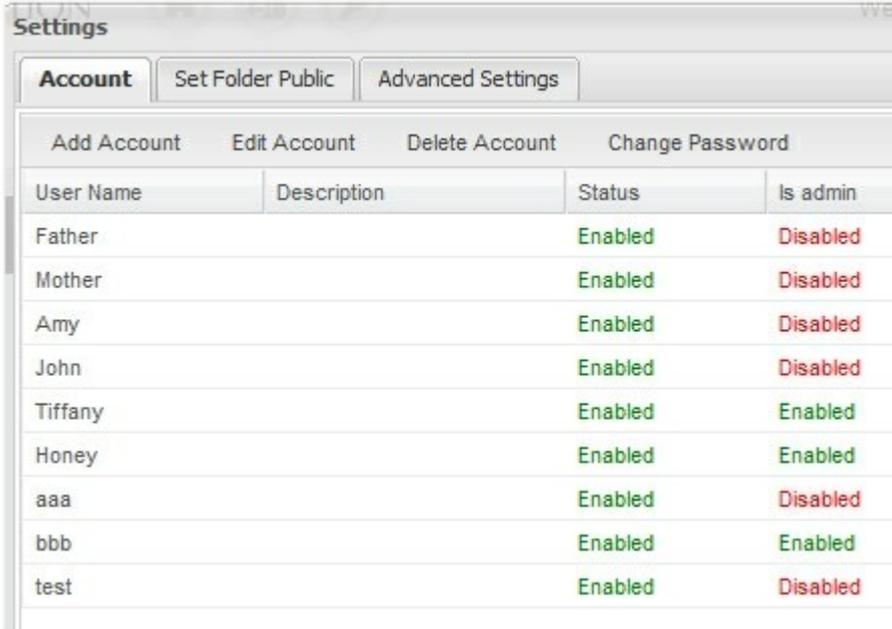
6. View a video

Click a video to view it by the web browser. To download the file, click "Download".



7. Settings

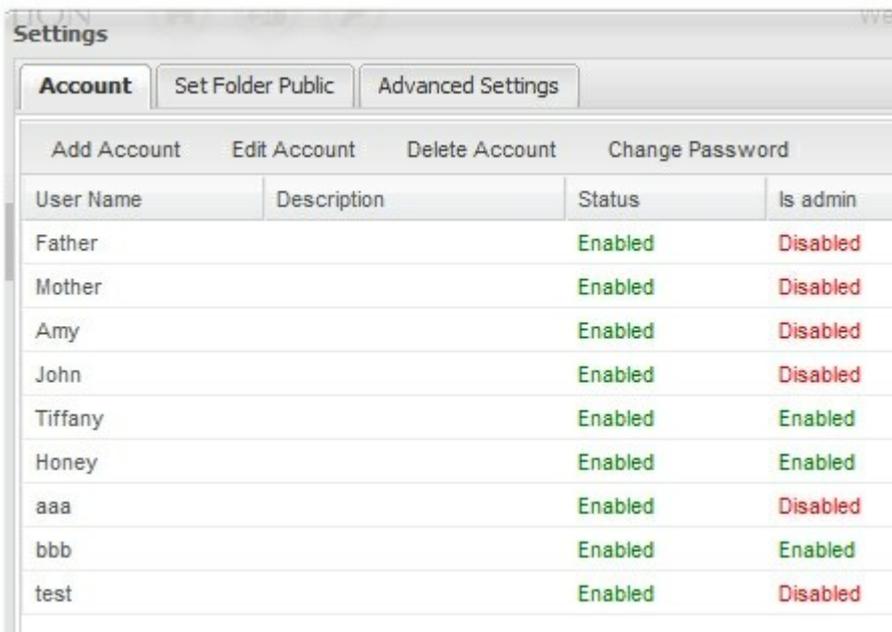
Click  to enter the Settings page.



User Name	Description	Status	Is admin
Father		Enabled	Disabled
Mother		Enabled	Disabled
Amy		Enabled	Disabled
John		Enabled	Disabled
Tiffany		Enabled	Enabled
Honey		Enabled	Enabled
aaa		Enabled	Disabled
bbb		Enabled	Enabled
test		Enabled	Disabled

7.1 Account

To create a user, click "Add Account" under the "Account" tab.



User Name	Description	Status	Is admin
Father		Enabled	Disabled
Mother		Enabled	Disabled
Amy		Enabled	Disabled
John		Enabled	Disabled
Tiffany		Enabled	Enabled
Honey		Enabled	Enabled
aaa		Enabled	Disabled
bbb		Enabled	Enabled
test		Enabled	Disabled

Enter the username (max 32 characters), password (1-16 characters), and description (max 127 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 username only supports A-Z, a-z, 0-9, dash (-), and underscore (_).
 - The password only supports A-Z, a-z, 0-9, -, !, @, #, \$, %, _.

Account | Set Folder Public | Advanced Settings

Add a New Account:

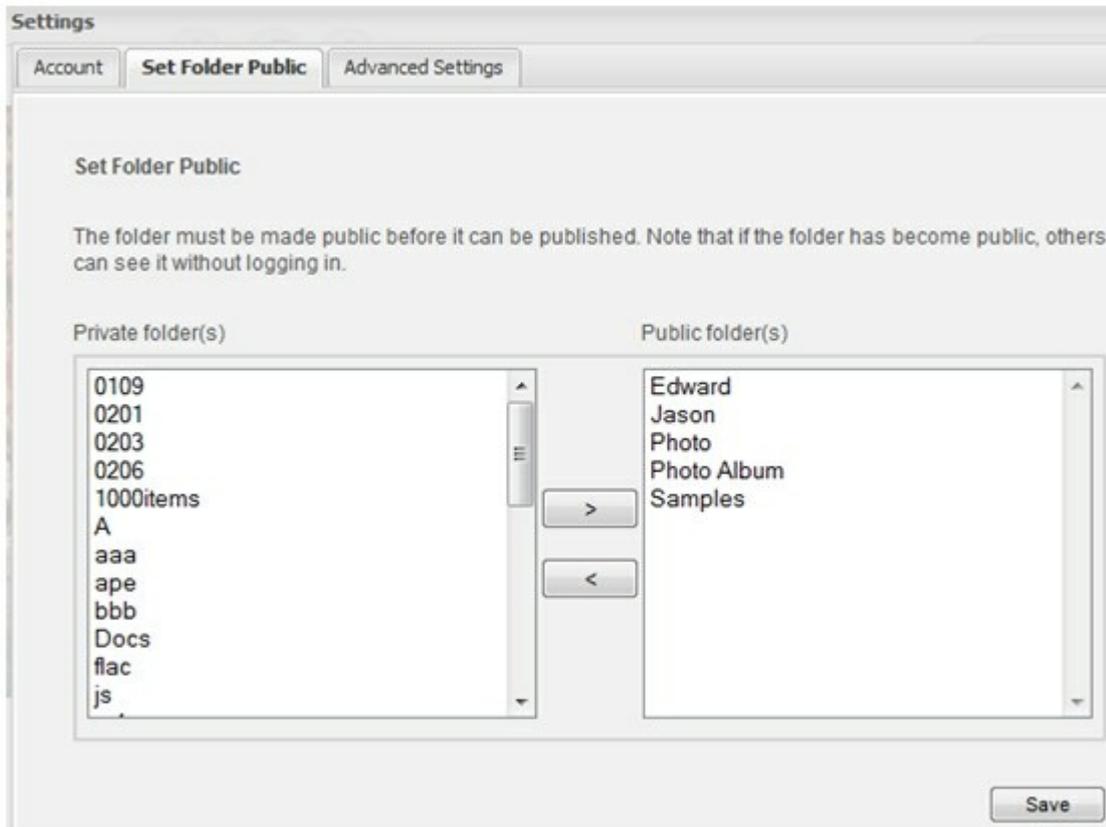
Name: john
Password: ●●●●●●
Verify Password: ●●●●●●
Description: friend
Status: Enabled Is admin

Inaccessible Folder: Jason, js, m4a, mp3 to aac, pdf
Accessible Folder: Music

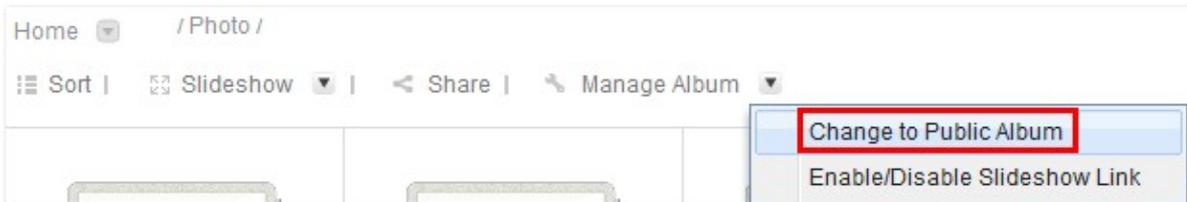
Save | Cancel

7.2 Set folder public

All the folders in the 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.

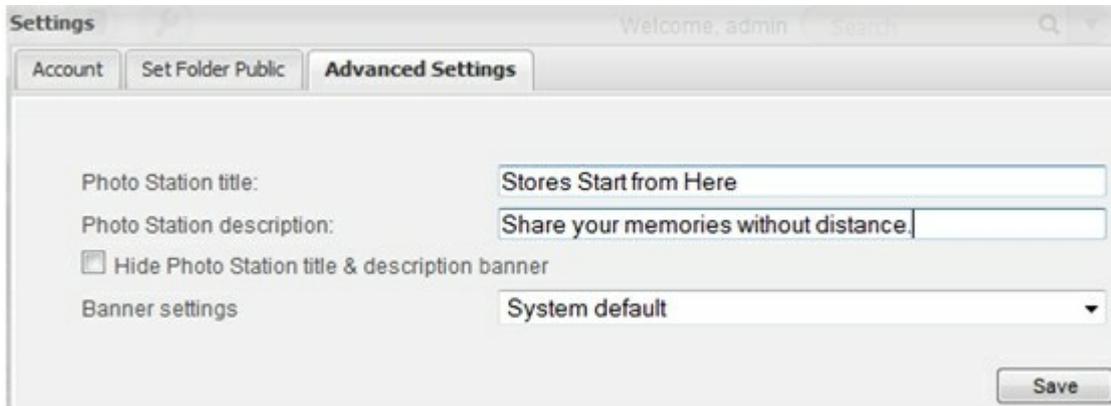


An album can also be changed to public or private by clicking .

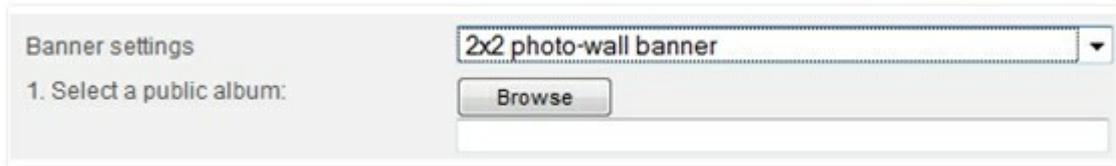


7.3 Advanced settings

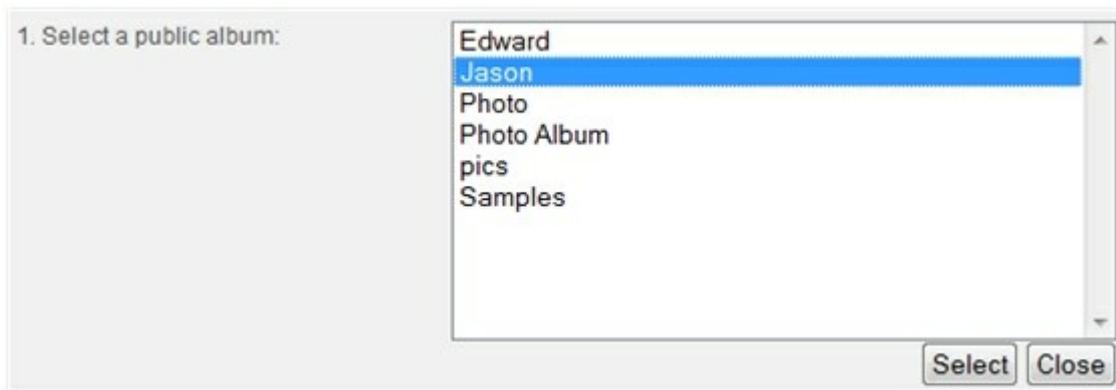
Customize the banner of the Photo Station on the home page in "Advanced Settings".



1. Enter the title (max 35 characters) and description (max 120 characters) of the 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".

Advanced Search

Search Type & Range

Type:

Range:

Search conditions

Album or File name:

Title:

Description:

Date photo taken:

From: 

To: 

Date file created:

From: 

To: 

7.4 Music Station

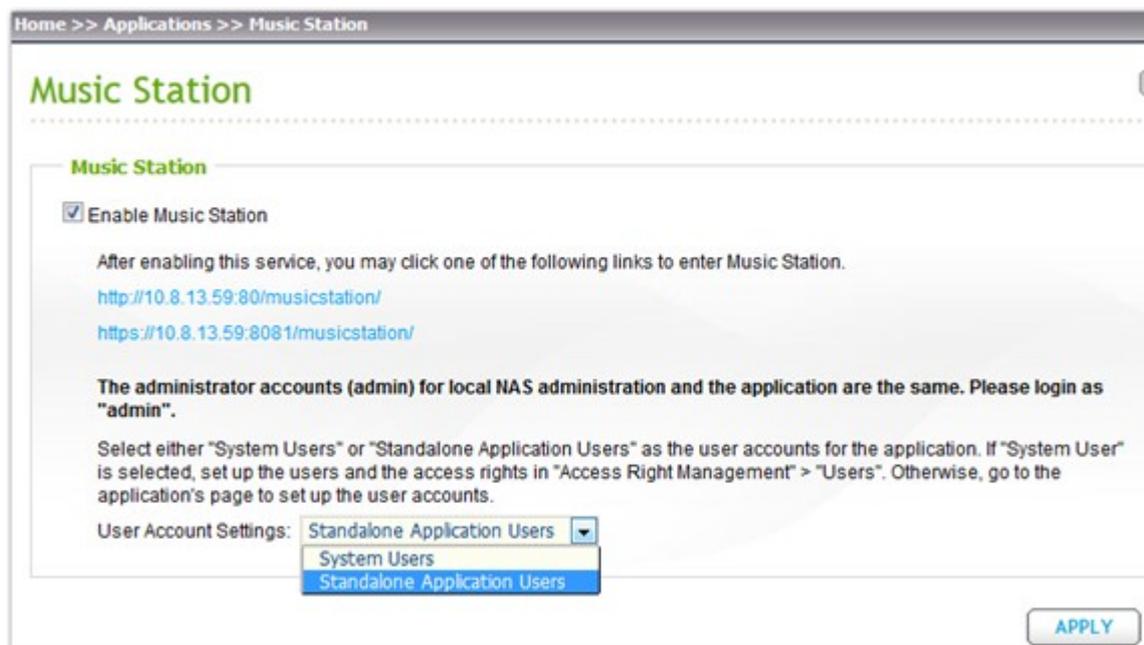
The Music Station is a web-based application for users to play the music files on the NAS or a media server, or listen to thousands of Internet radio stations by a web browser or a local USB speaker connected to the NAS. Music alarms can also be set with the local playback feature.

Before getting started

1. Specify the user account settings

The Music Station is enabled by default. Before using this application, login the NAS as "admin" and go to "Administration" > "Applications" > "Music Station".

Select either "System Users" or "Standalone Application Users" (default) for the user account settings. When "System Users" is selected, the local NAS accounts will be used for the application. You can create the user accounts in "Access Right Management" > "Users". To use dedicated user accounts for the application, select "Standalone Application Users". The user accounts can be created and managed after logging in the application under "Settings".



2. Upload music files to the NAS

Upload the music files and folders to the network share "Multimedia" or "Qmultimedia" of the NAS. The folders uploaded to the Music Station are for private viewing by default and can only be managed by the administrator or authorized admin groups.

Note: The Music Station only supports audio files in MP3, OGG, WAV, AIFF, AU, FLAC, M4A, APE format.

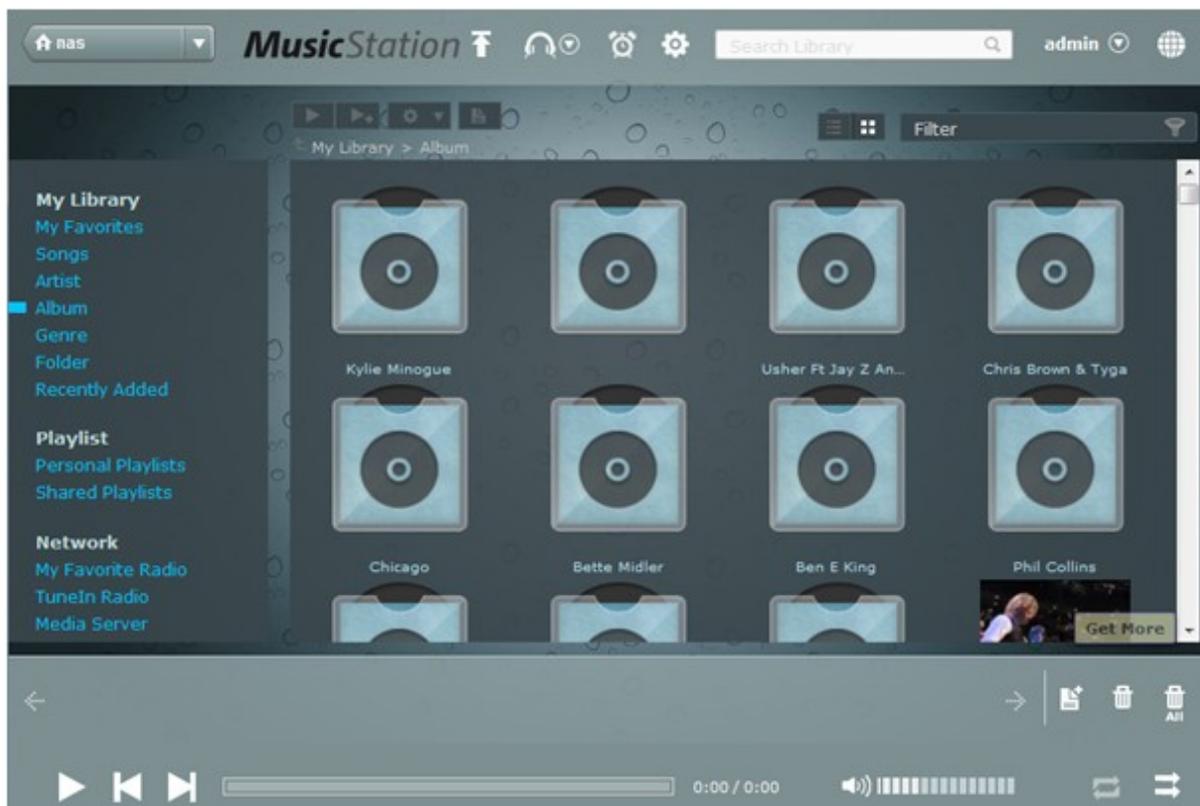
Login the Music Station

Connect to the Music Station from the login portal of the NAS or enter <http://NAS IP/musicstation> in a web browser (Internet Explorer, Mozilla Firefox, or Google Chrome).



Note:

- The admin login information of the Music Station is the same as that of the NAS web administration.
- Login to the application from the login portal of the NAS will be disabled when standalone user accounts are in use, except for "admin".



The three main sections of the Music Station are listed on the left panel. The sections include My Library, Playlist, and Network.

1. My Library:

All the folders and supported music files on the Multimedia/Qmultimedia folder of the NAS are shown under My Library. Select to browse the files by My Favorites, Songs (individual files), Artist, Album, Genre, Folder, or Recently Added.

Note: The Music Station only supports audio files in MP3, OGG, WAV, AIFF, AU, FLAC, M4A, APE format.

Icon	Description
	Play the music file(s) selected.
	Add one or more music files or an album to the now playing list.
	Add to My Favorites: Add one or more music files to My Favorites. Song Info: View the information of a music file.
	Add to Playlist: Add one or more music files to an existing playlist. Save as Playlist: Replace an existing playlist.

	Save as New Playlist: Create a playlist and specify if it is a personal or shared playlist.
--	---

2. Playlist:

The Music Station offers two types of playlists:

- Personal playlists: The playlists that can be viewed and played by the user only. Maximum 200 playlists can be created.
- Shared playlists: The playlists that can be viewed and played by all the users of the Music Station. Maximum 200 playlists can be created.

Each playlist can contain maximum 600 items, including the music files on the NAS or a media server, TuneIn Radio stations, and Internet radio stations

Icon	Description
	Play the music file(s) selected.
	Add one or more music files or an album to the now playing list.
	Add to My Favorites: Add one or more music files to My Favorites. Remove: Remove the music file from the playlist. Song Info: View the information of a music file.
	Add to Playlist: Add one or more music files to an existing playlist. Save as Playlist: Replace an existing playlist. Save as New Playlist: Create a playlist and specify if it is a personal or shared playlist.
	Save the settings.

3. Network:

Users can listen to the Internet radio stations or play the music files on any UPnP media servers.

My Favorite Radio: User's favorite Internet radio stations added by entering the radio URL or by searching TuneIn Radio. Maximum 1024 items are supported. Note that the type of the radio stations must be MP3.

Icon	Description
	Play the radio station(s) selected.
	Add one or more radio stations to the now playing list.
	Add an Internet Radio Edit Internet Radio Settings Delete an Internet Radio
	Add to Playlist: Add one or more radio stations to an existing playlist. Save as Playlist: Replace an existing playlist. Save as New Playlist: Create a playlist and specify if it is a personal or shared playlist.

TuneIn Radio: Search for the stations available on TuneIn Radio.

Icon	Description
	Play the radio station(s) selected.
	Add one or more radio stations to the now playing list.
	Add one or more radio stations to My Favorite Radio.
	<p>Add to Playlist: Add one or more radio stations to an existing playlist.</p> <p>Save as Playlist: Replace an existing playlist.</p> <p>Save as New Playlist: Create a playlist and specify if it is a personal or shared playlist.</p>



Media Server: Displays the UPnP media servers (maximum 2000) available on the local network. Only the music files supported will be shown.

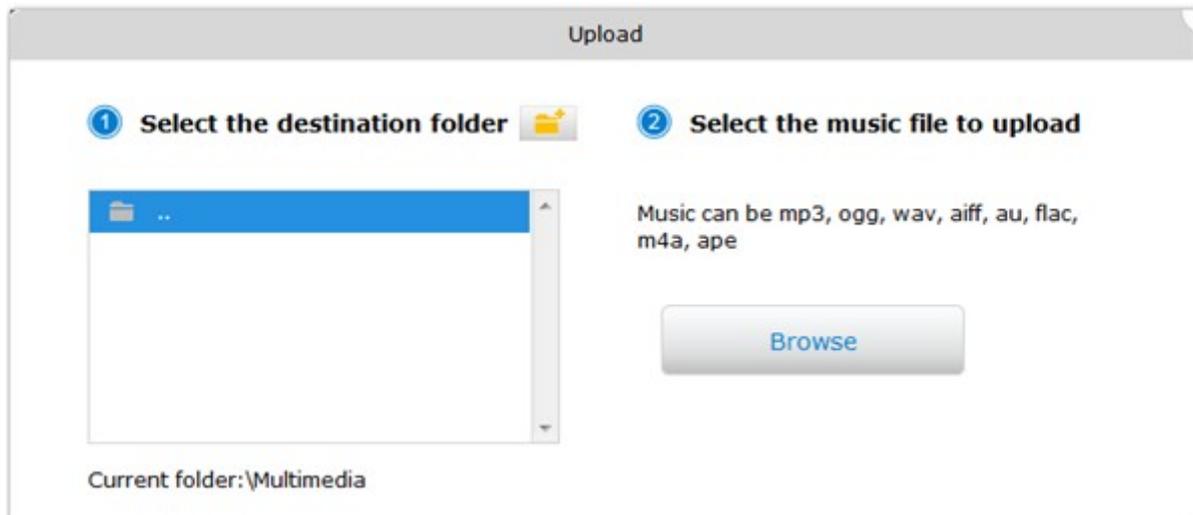
Icon	Description
	Play the music file(s) selected.
	Add one or more music files or an album to the now playing list.
	Add to My Favorites: Add one or more music files to My Favorites.
	Add to Playlist: Add one or more music files to an existing playlist. Save as Playlist: Replace an existing playlist. Save as New Playlist: Create a playlist and specify if it is a personal or shared playlist.

Upload music by the web interface of the Music Station:



To upload music to the Music Station, click .

Specify the destination folder and select the music files to upload.



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.



Search music library

To search for a music file or an album, enter the keyword in the search box and click .



Before starting to play the music, click  to select the playing mode.

- Streaming Mode: Stream the music files to the computer or the device and play them by the web browser.
- NAS USB Mode: Play the music files by the USB speaker connected to the NAS.



Player

Icon	Description
	Play.
	Pause.
	Play the previous item.
	Play the next item.
	Adjust the volume.
	No repeat, repeat once, or repeat all.
	Shuffle on/off.
	Save the now playlist list to replace an existing playlist or as a new one.
	Delete an item on the playlist.
	Delete all items on the playlist.

Play music files

Browse the contents under "My Library", "Playlist", or "Network".

Select an item and click  (Play now) or  (Add selected entries to now playing list), or double click the item to play it immediately, or drag and drop the item to the now playing list.

To play multiple files, press and hold the Ctrl key and click to select the files, or drag the mouse to

select multiple items. Then click  (Play now) or  (Add selected entries to now playing list), or drag and drop the items to the now playing list.

Play a folder

Select a folder and click  (Add Selected Entries to Playlist) or drag and drop the folder to the now playing list.

Note: If a folder contains more than 100 music files, only the first 100 files will be added to the playlist.

Music Alarm

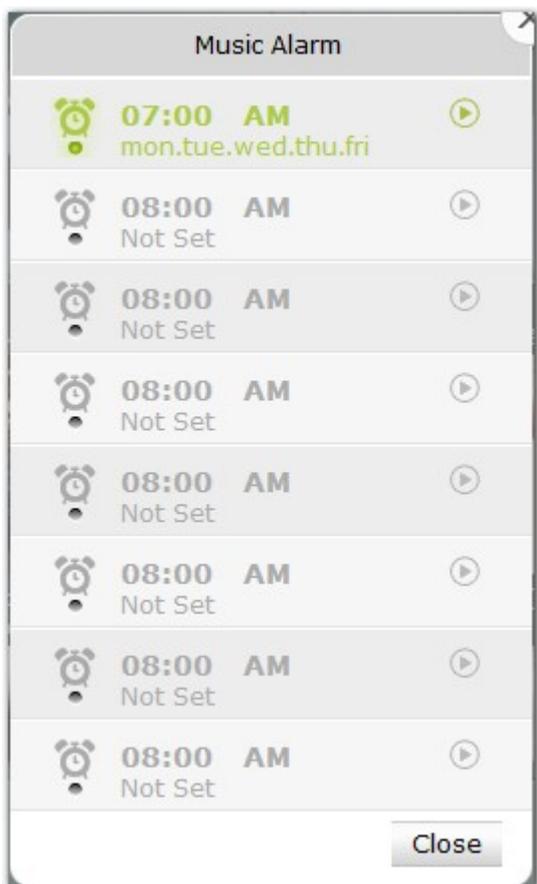
The Music Station supports setting music alarm in local playback mode. To use this function, a USB speaker or USB soundcard must be connected to the NAS.

Set music alarm

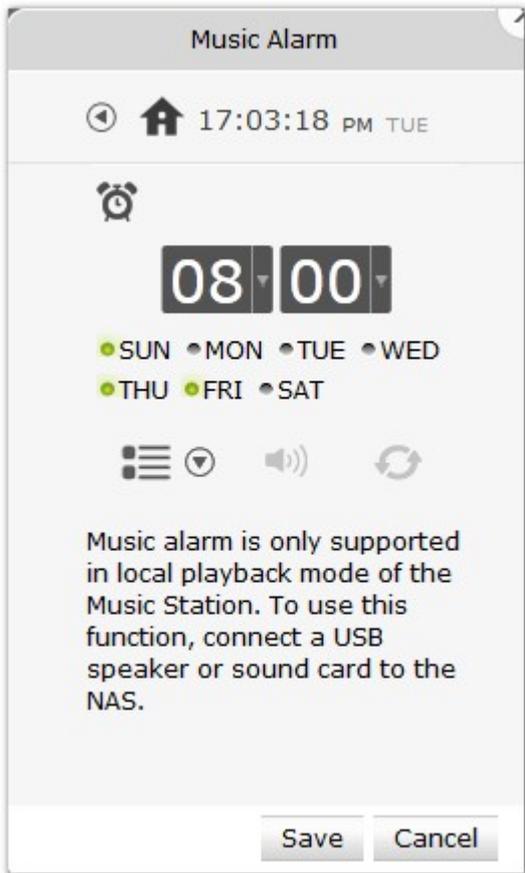
1. Click .



2. Click a schedule.



3. Set up the alarm schedule.



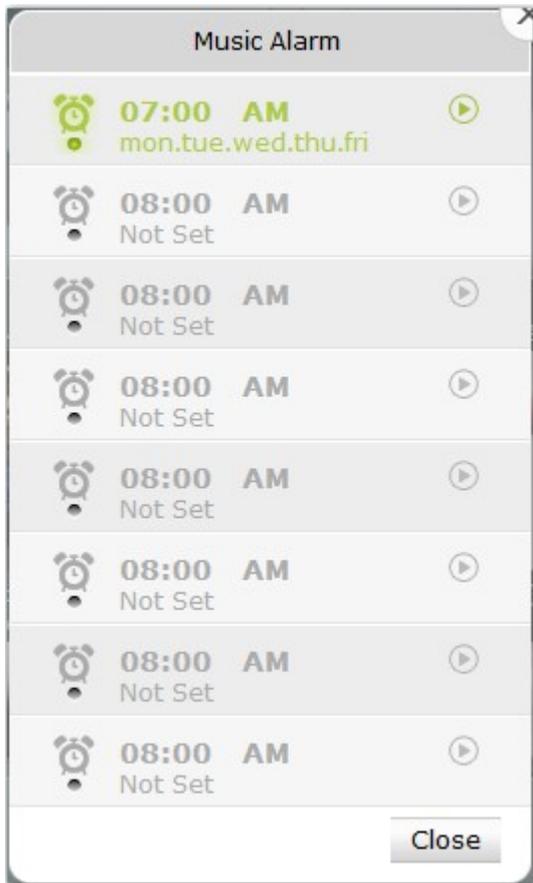
4. Click  to select to use the default alarm or a playlist on the Music Station.
5. Click  to adjust the alarm volume.
6. Click  (Repeat) to play the playlist repeatedly when the alarm is on.
7. Click "Save".

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 for two seconds.

Music Library and Account Management

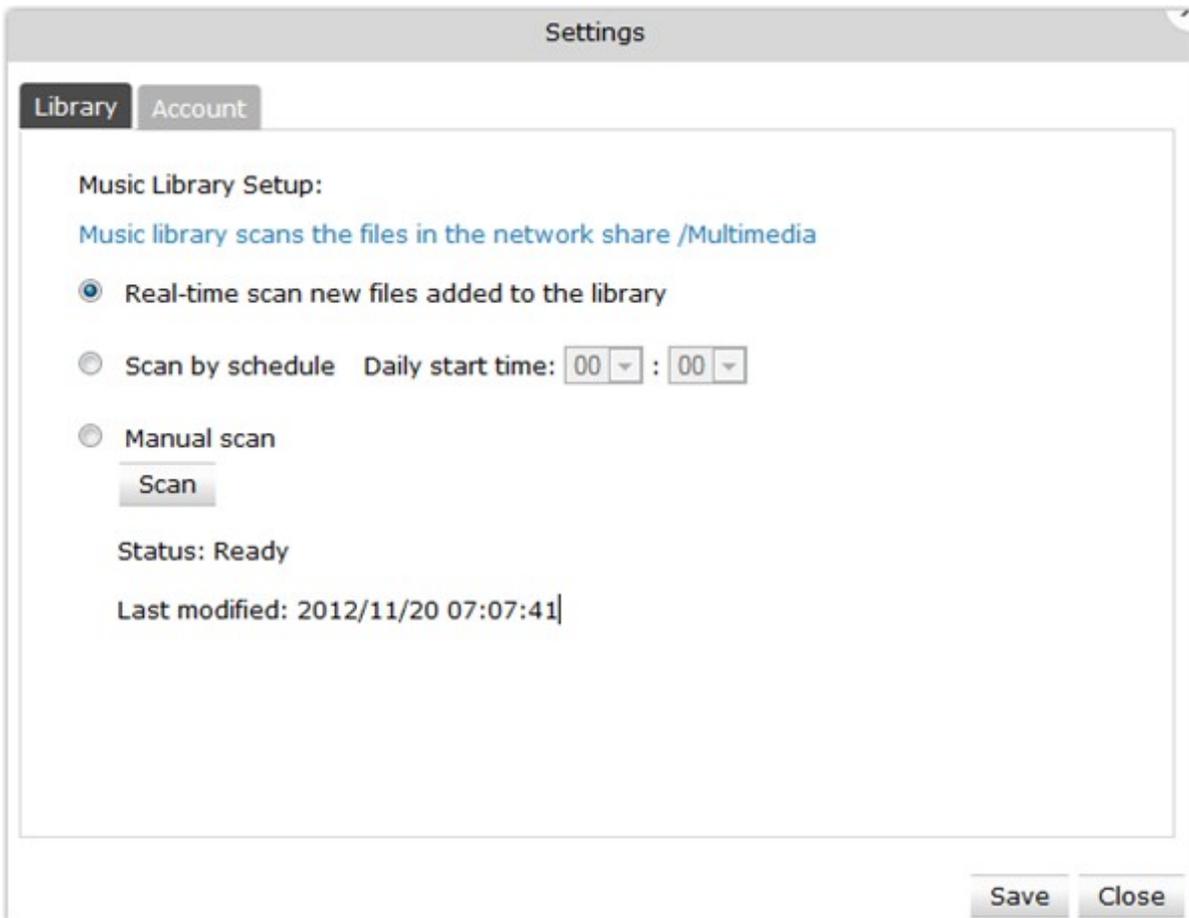
A. Scan music library

To specify when to update the music library, click .



Under the "Library" tab, select when the music library will be updated.

- Real-time scan: Update the music library immediately when new files are added.
- Scan by schedule: Specify the time to update the music library daily.
- Manual scan: Click "Scan" to update the music library.

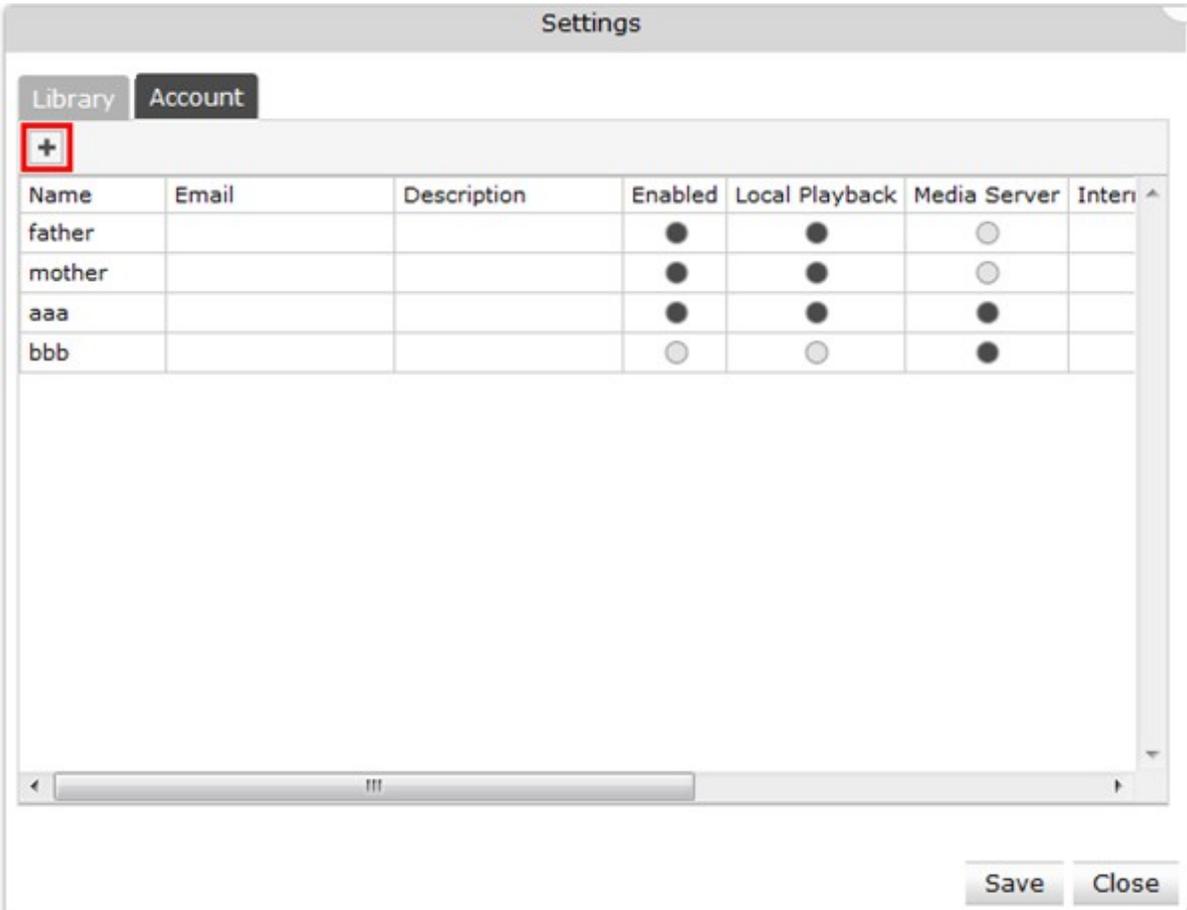


B. Account Management

1. Click .



2. To create an account, click + under the "Account" tab.



3. Enter the username (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.

The screenshot shows a 'Settings' dialog box with two tabs: 'Library' and 'Account'. The 'Account' tab is selected. Under the 'Add Account' section, there are five text input fields: 'Name', 'Password', 'Verify Password', 'Email', and 'Description'. The 'Name', 'Password', and 'Verify Password' fields are marked with a red asterisk and the text '* Required Fields'. Below the input fields, there are six radio button options arranged in two columns: 'Enabled' (selected), 'Local Playback', 'Edit Music Info' in the first column; and 'Internet Radio', 'Media Server', 'Manage Playlist' in the second column. At the bottom right of the dialog box, there are 'Save' and 'Cancel' buttons.

4. Enable or disable the account and grant the privileges.

- Local Playback: Allow the user to play the music files via local playback (NAS USB mode).
- Edit Music Info: Allow the user to edit the music information.
- Internet Radio: Allow the user to access the Internet radio stations and edit the settings.
- Media Server: Allow the user to access the Media Server contents.
- Manage playlist: Allow the user to edit the shared playlists.

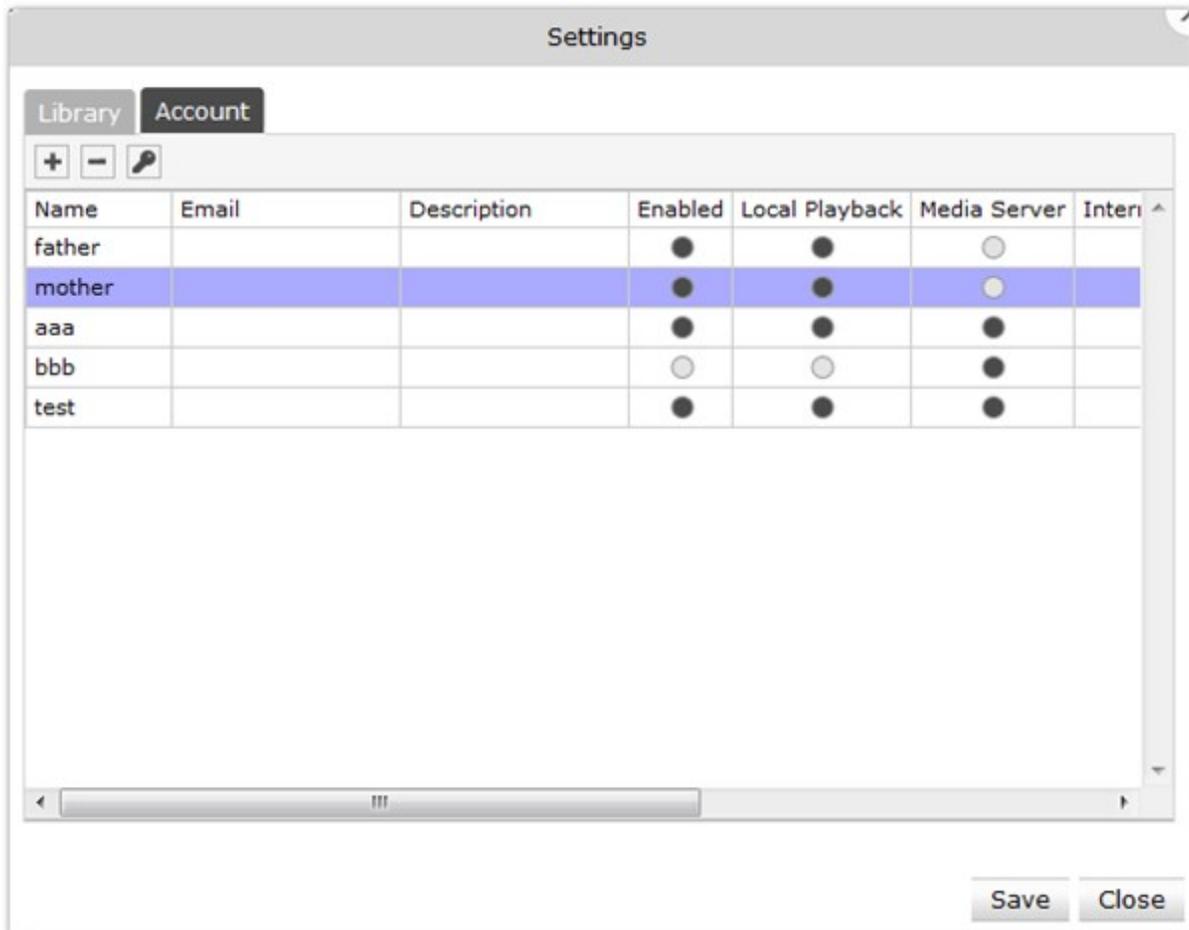
5. Click "Save".

Note: If a folder contains more than 100 music files, only the first 100 files will be added to the playlist.

Edit an account



To edit an account, click  and browse to the "Account" tab. Edit the account settings on the table.

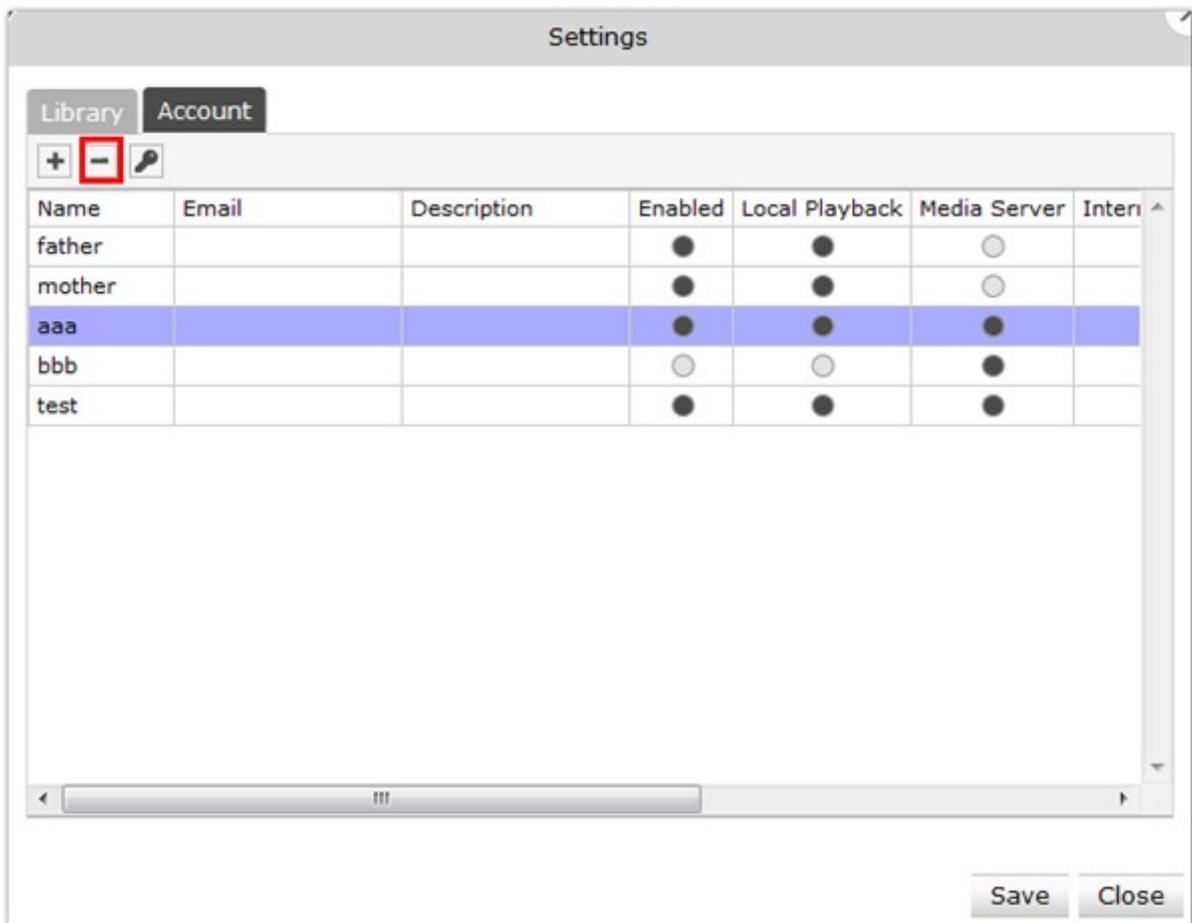


The screenshot shows a window titled "Settings" with two tabs: "Library" and "Account". The "Account" tab is active. Below the tabs are three icons: a plus sign, a minus sign, and a key icon. A table with the following columns is displayed: Name, Email, Description, Enabled, Local Playback, Media Server, and Inter. The "mother" row is highlighted in blue. Below the table is a large empty text area. At the bottom right of the window are "Save" and "Close" buttons.

Name	Email	Description	Enabled	Local Playback	Media Server	Inter
father			<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
mother			<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
aaa			<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
bbb			<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
test			<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	

Delete an account

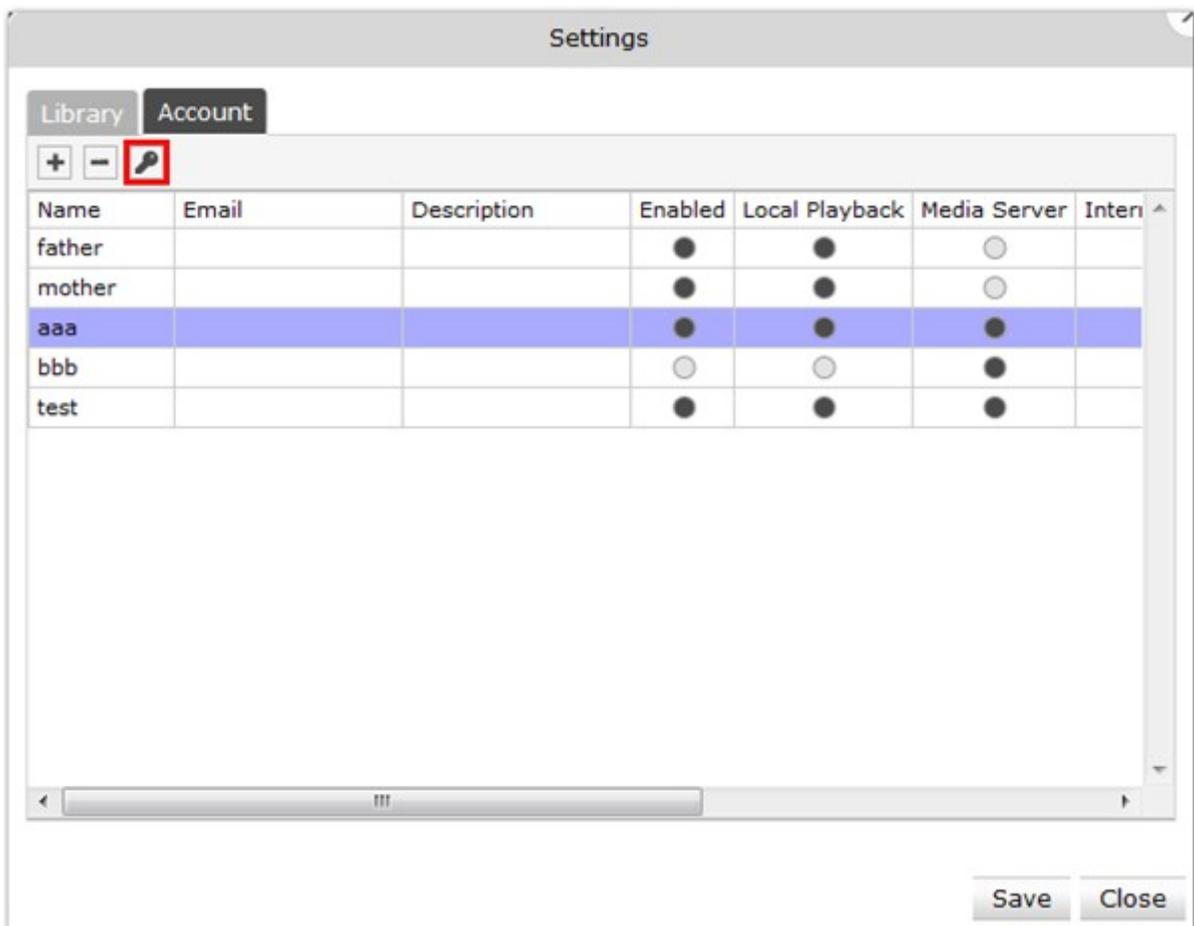
To delete an account, click  and browse to the "Account" tab. Select an account to delete and click .



Change password



To change the password of an account, click  and browse to the "Account" tab. Select an account and click .



The screenshot shows a "Settings" dialog box with two tabs: "Library" and "Account". The "Account" tab is active. In the top toolbar, there are three icons: a plus sign, a minus sign, and a key icon. The key icon is highlighted with a red square. Below the toolbar is a table with the following data:

Name	Email	Description	Enabled	Local Playback	Media Server	Inter
father			●	●	○	
mother			●	●	○	
aaa			●	●	●	
bbb			○	○	●	
test			●	●	●	

At the bottom right of the dialog box, there are two buttons: "Save" and "Close".

Enter the new password and click "Save".

Settings

Library **Account**

Change Password

Name : aaa

Password :

Verify Password :

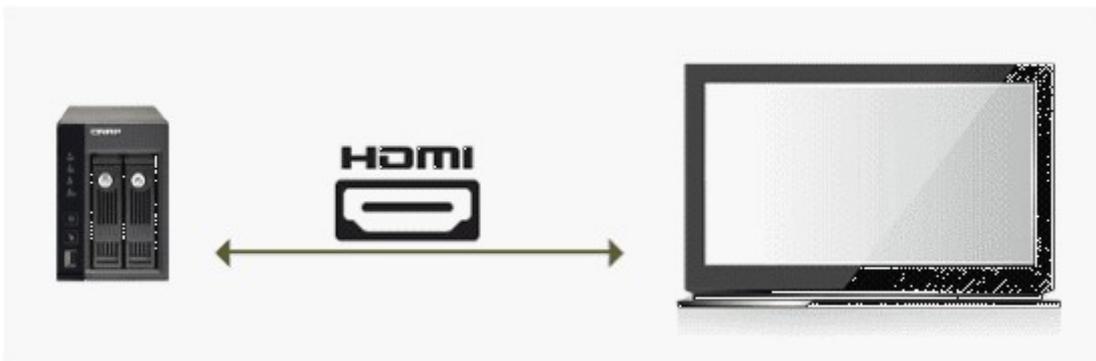
7.5 HD Station

The HD Station is a platform where the famous XBMC application or Chrome browser can be installed to let you directly play back your NAS multimedia contents or browse the internet websites on the TV screen thru the HDMI interface.

Note: Currently, the HD Station is supported by the TS-x69L, TS-x69 Pro, TS-x70 and TS-x70 Pro Turbo NAS models.

Create your lovely media environment by following the steps below:

1. Setting up the environment of the HD Station: Connect the NAS to the HDMI TV with a HDMI cable



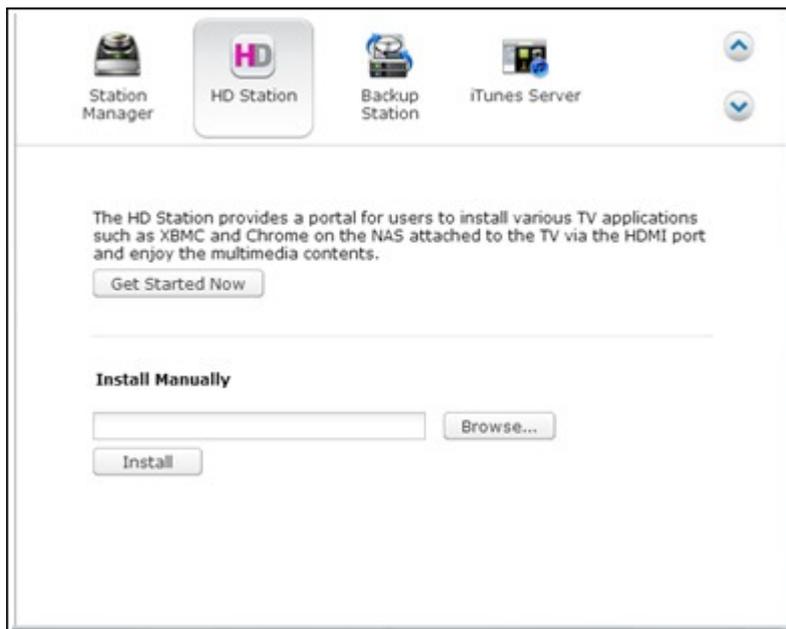
Remote controller: There are 4 different ways to control the HD Station.

- A. QNAP remote controller
- B. MCE remote controller
- C. USB keyboard or mouse
- D. Qremote: QNAP remote app, exclusively designed for the HD Station.

Note: If you want to use the Chrome to browse an internet website, you are required to use the mouse function on the Qremote or use the USB mouse directly connected to the NAS.

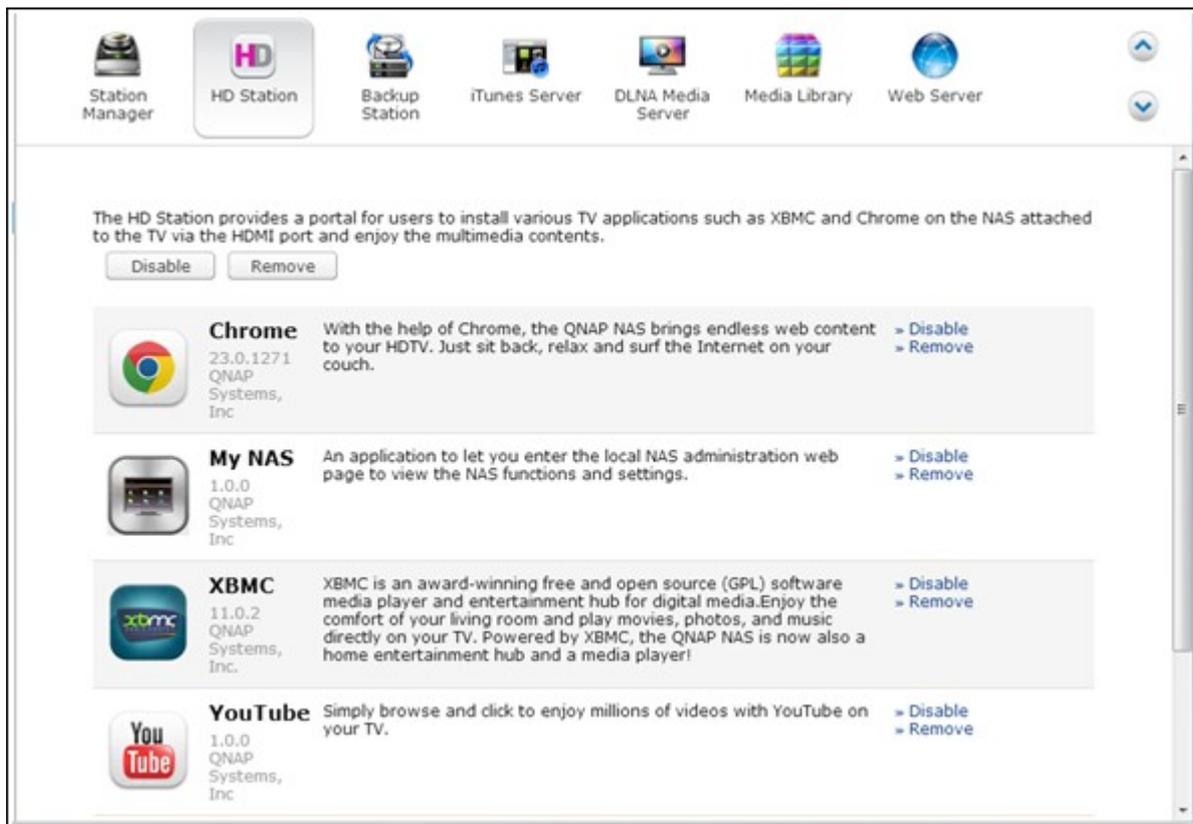
2. Installing the HD Station:

Go to "Applications" > "HD Station" and click the "Get Started Now" button. Then, the system will install the HD Station automatically.



3. Choosing the applications to install.

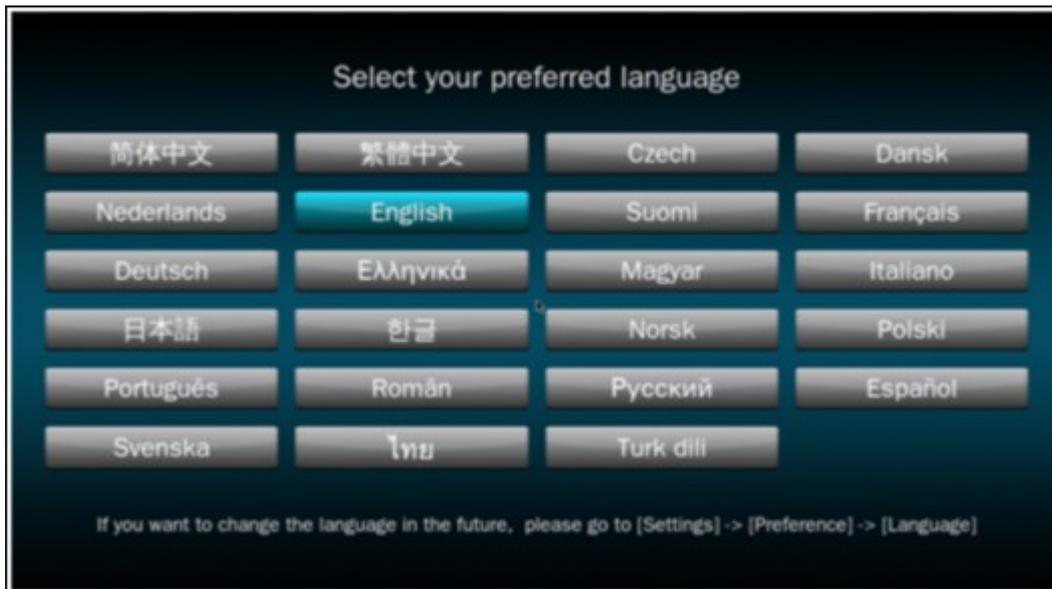
- HD Station: The HD Station portal, which allows you to use the following applications on the TV screen.
- XBMC: An application for you to operate and enjoy your multimedia data on the TV screen.
- Chrome: With the help of Chrome, the QNAP Turbo NAS brings endless web content to your HDTV. Just sit back, relax, and surf the Internet on your couch.
- YouTube: Simply browse and click to enjoy millions of YouTube videos on your TV.
- My NAS: An application for you to enter the local NAS administration web page to view the NAS functions and settings.



Note:

- Keeping staying at XBMC, Chrome, or other applications could affect the hard drive hibernation of the NAS. Please always exit the application and return to the HD Station portal.
- Press the power button on the remote control for 6 seconds anytime to exit an application.
- Press the one touch copy button on the NAS for 6 seconds to restart the HD Station.
- For the best HD Station experience, QNAP recommends upgrading the memory on your TS-x69 Series Turbo NAS to 2GB or more.
- To use the AirPlay function provided by XBMC, please upgrade the memory on your TS-x69 Series Turbo NAS to 2GB or more.
- The HD Station will restart when formatting an USB external device.
- The first time XBMC is launched, it will index the "Multimedia" shared folder and it may consume a lot of system resources if the folder contains a lot of multimedia files.

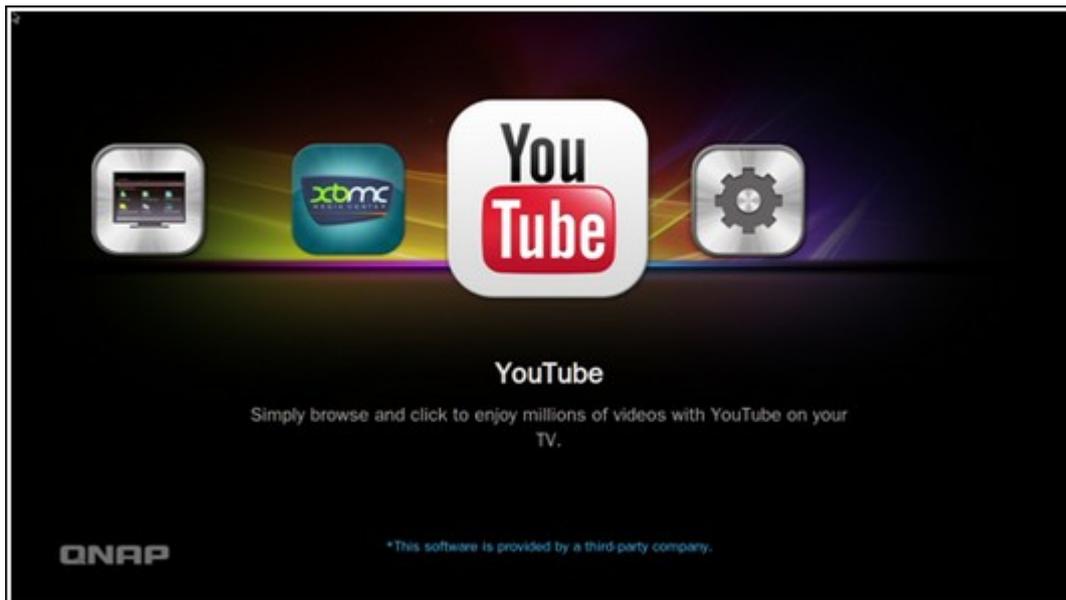
After installation, please choose your preferred language on the TV screen.



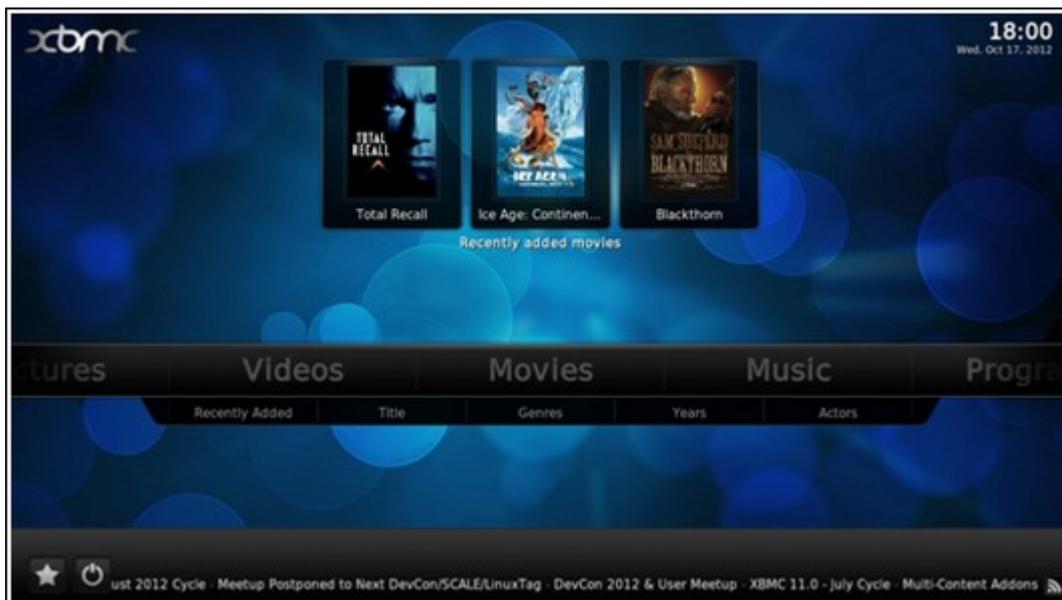
After selecting the language, you will see the HD Station portal as shown below.



- 4. Enjoying the HD Station: At the HD Station portal, simply choose the application you want to use to start enjoying the service.**



Enjoy the comfort of your living room and play movies, photos, and music directly on your TV by XBMC or other applications.



Take a picture with your smart phone and watch on your TV

The first part is done by Qfile on your phone:

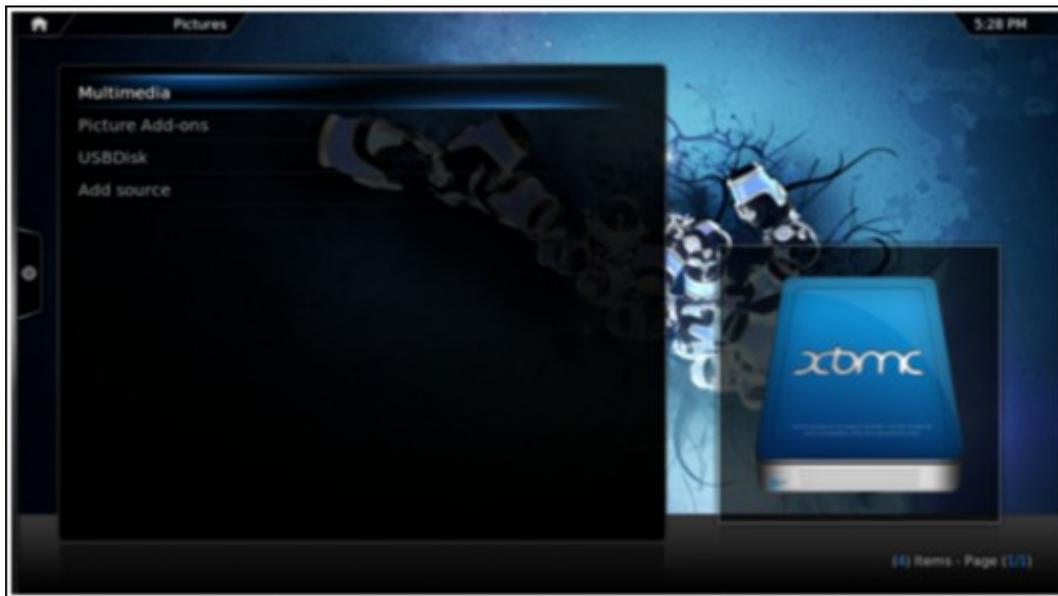
- a. Use Qfile to browse your NAS.
- b. Choose the multimedia shared folder.
- c. Select the upload function.
- d. Take a picture and upload it to the NAS.

The second part is performed by the HD Station on your TV:

- e. Turn on your TV and choose XBMC.
- f. Choose "Pictures" like below:



- g. Select the "Multimedia" folder.

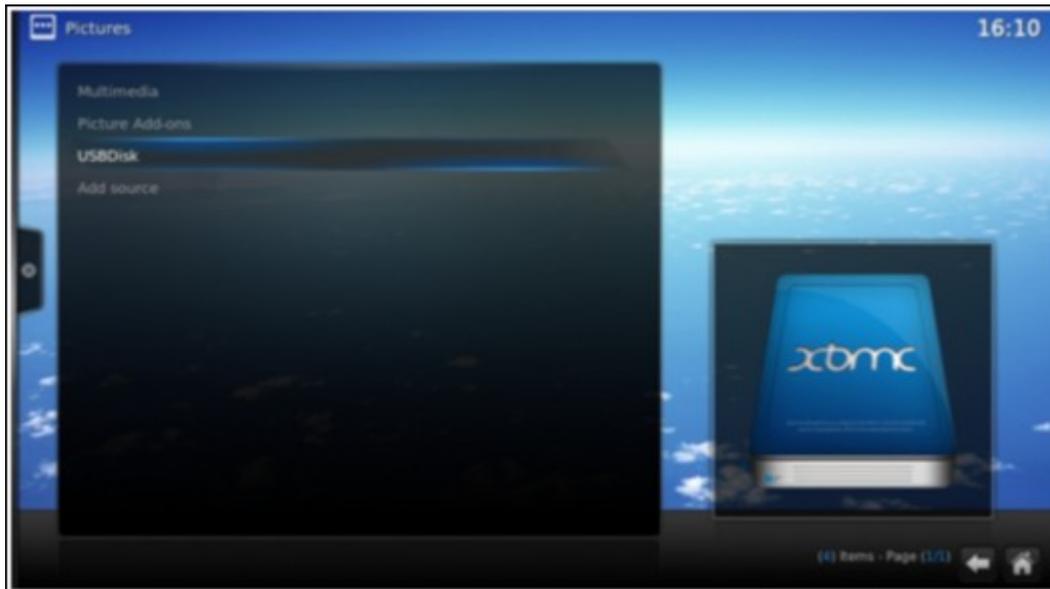


h. Double click the picture you just uploaded.

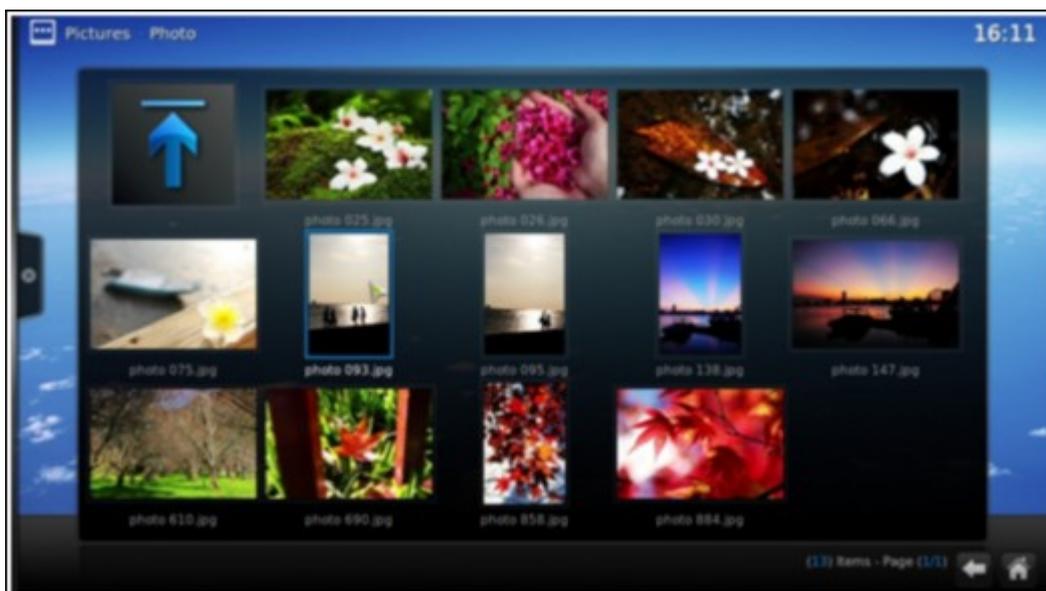


Viewing photos on your USB device or camera

- a. Connect your USB device or camera to the USB port of your NAS.
- b. Choose "Pictures".
- c. Choose "USB Disk".



- d. Select the photo you want to view.



Importing media contents to your NAS

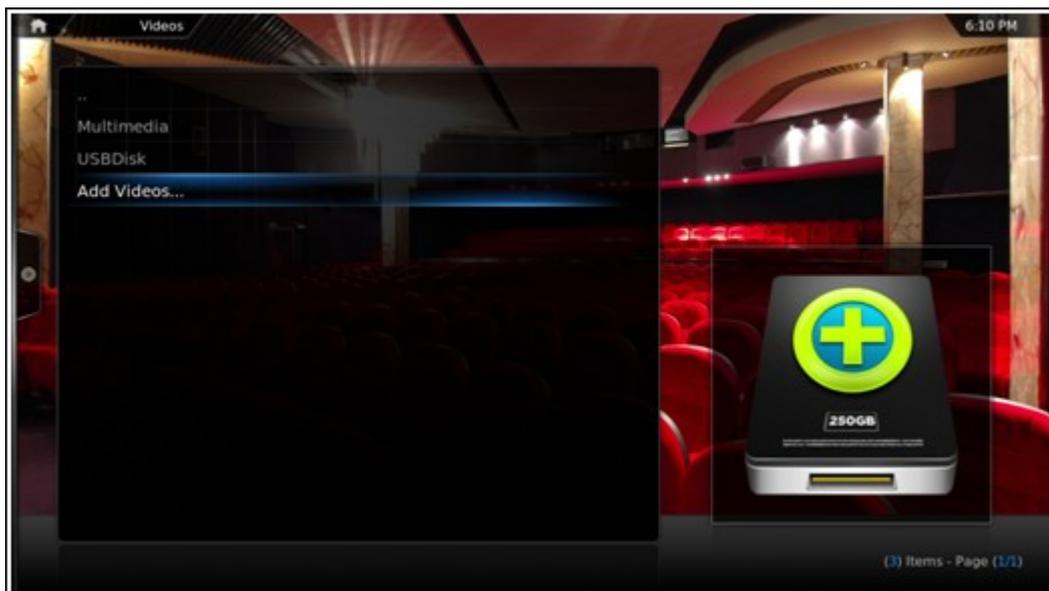
Use one of the several types of network protocols (Samba, AFP, FTP, and NFS) to save the media content files in the "Multimedia" or "Qmultimedia" shared folder, or copy them from an external USB or eSATA device.

To browse the media contents in different folders other than the default "Multimedia" shared folder, perform the following steps:

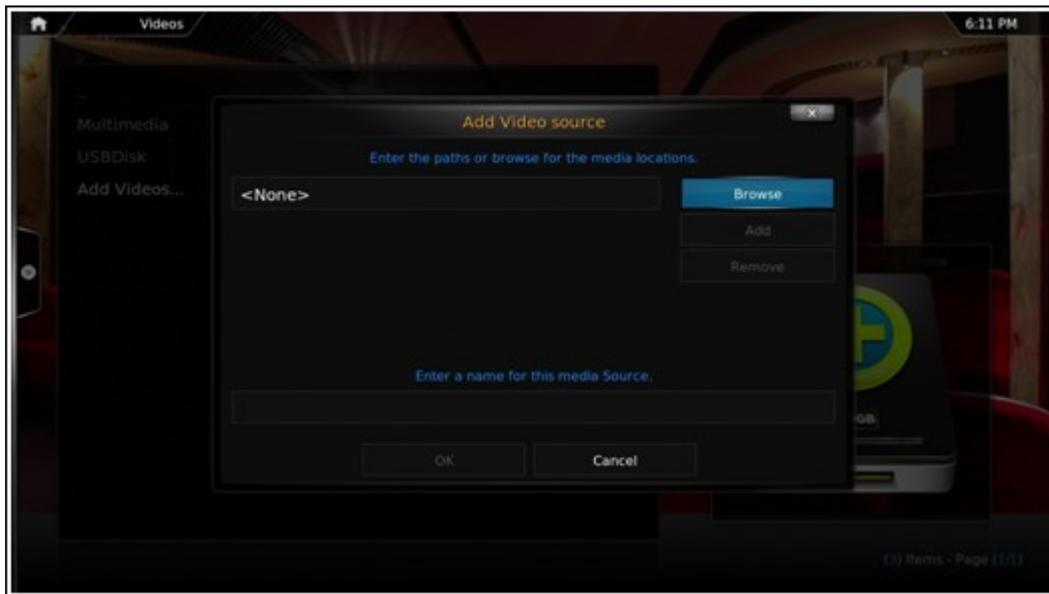
- a. Choose "Files" under "Videos".



- b. Choose "Add Videos".



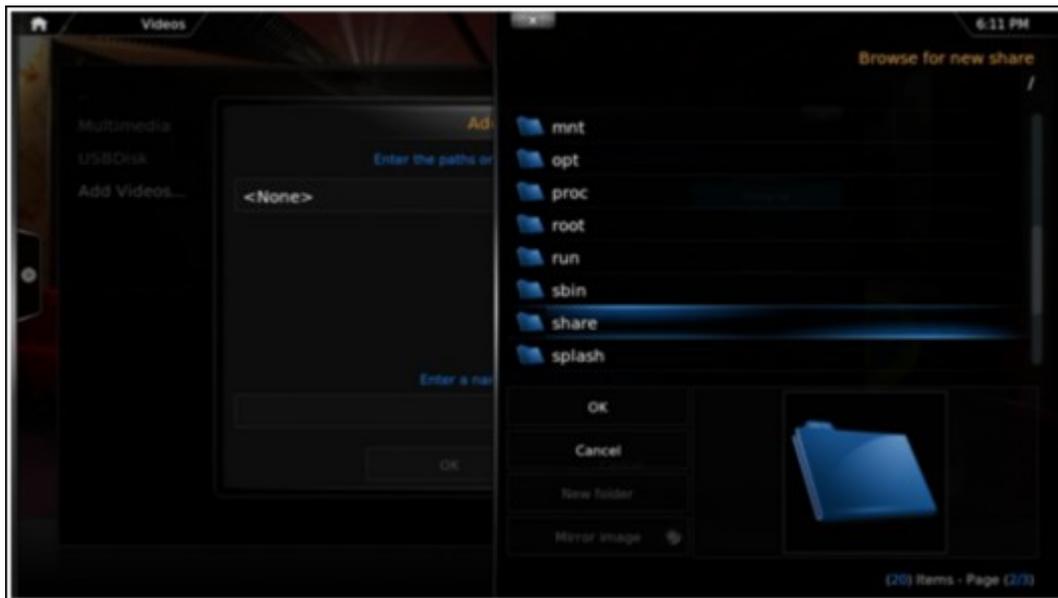
- c. Click "Browse".



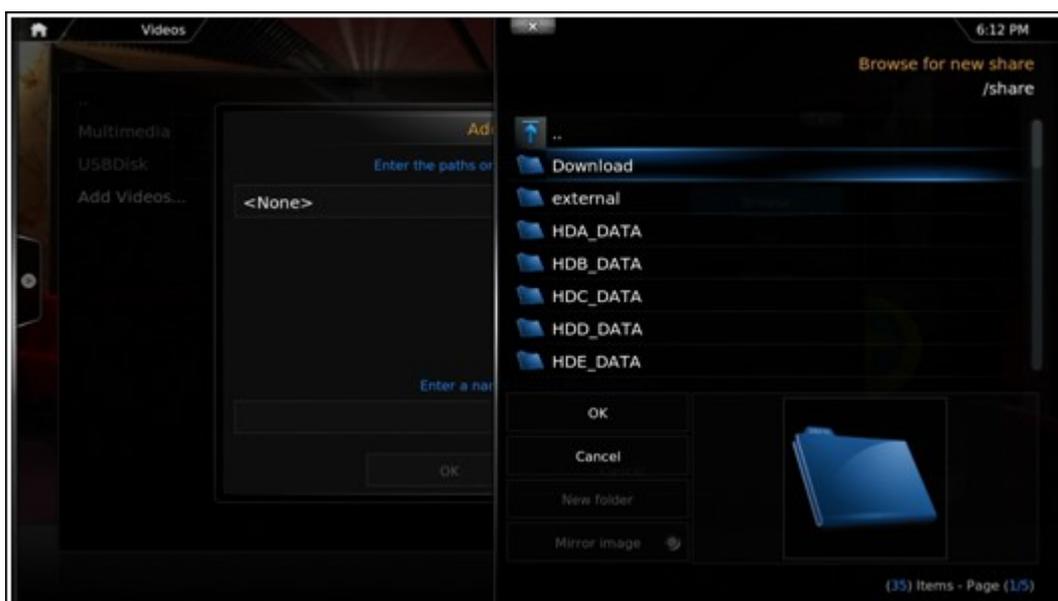
d. Choose "Root filesystem".



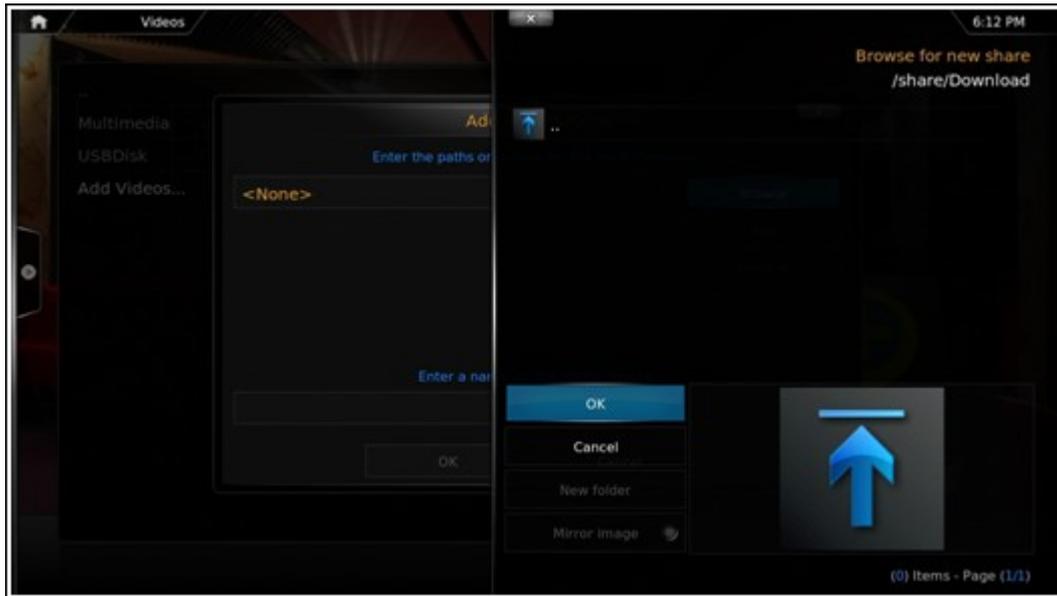
e. Choose "share".



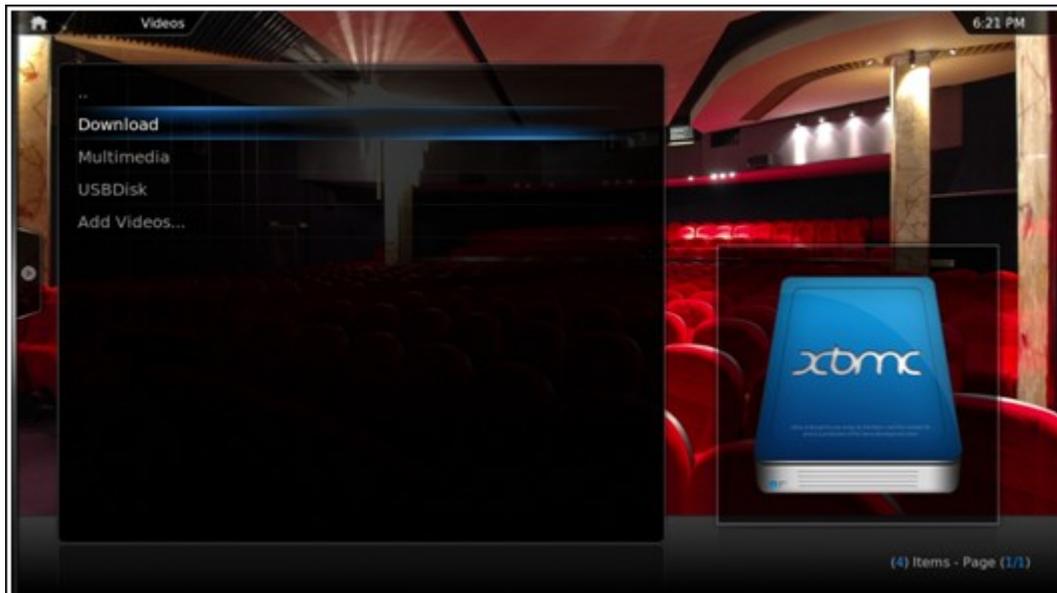
- f. If you want to add the "Download" shared folder, for example, choose "Download" like below. Otherwise, just choose the shared folder you would like to add as a video source.



- g. Click "OK" to add this source.



h. You will see the "Download" shared folder in the list.



Note:

- If you encounter any video playback quality issues with some video formats, you may enable the following settings on the XBMC: Go to "Setting" > "Video" > "Playback", and then enable "Adjust display refresh rate to match video" and "Sync playback to display".
- Depending on the data type, some files may not be playable.

Chrome

Select the Chrome application at the main page of the HD Station like below:



You may surf the web like using a web browser on your PC.

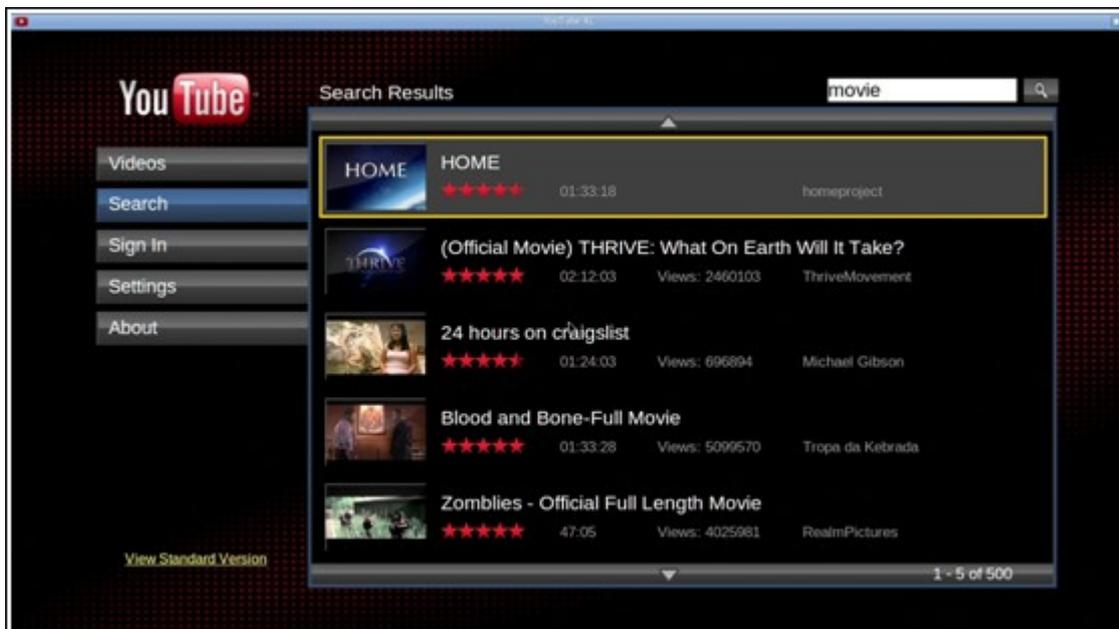


Note: In order to use this application, you are required to use the mouse function on the Qremote, or use the USB mouse directly connected to the NAS.



YouTube

Enjoy the YouTube contents via the HD Station.



MyNAS

Enter the local NAS administration web page to view the NAS functions and settings.

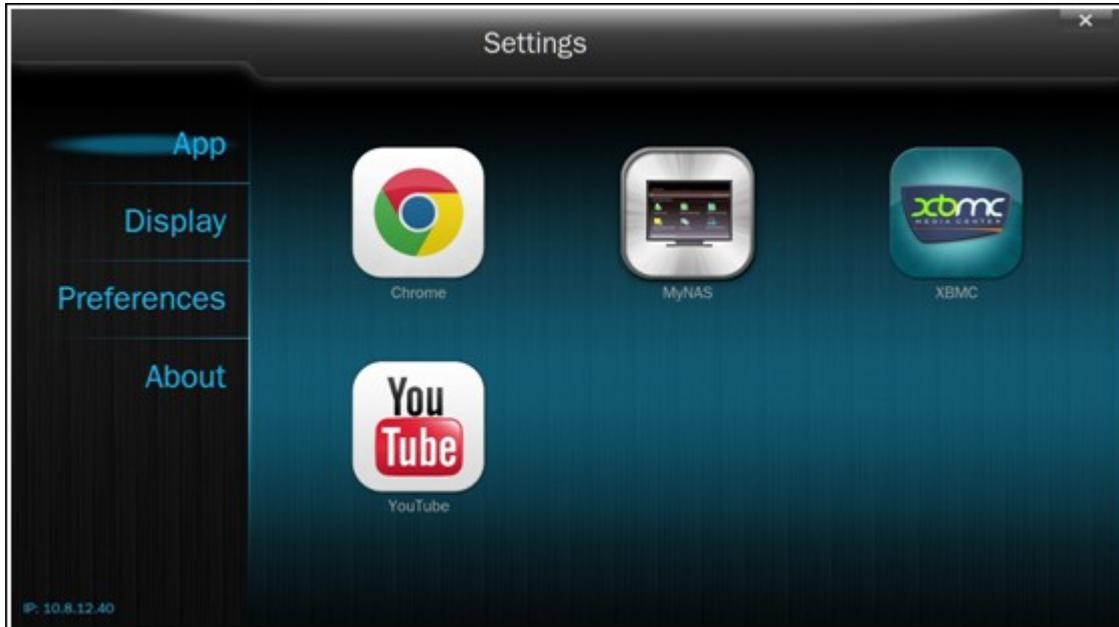


Configuring settings of the HD Station

Configure the HD Station by choosing "Settings" at the HD Station portal.



- i. App: The applications can be enabled or disabled in this feature.



- ii. Display: Here you may change the screen resolution and set up to turn off the screen after an amount of idle time.



- iii. Preferences: Here you may change the language or type of remote control and audio output. The default setting is HDMI. If you have a USB sound card installed, you can choose that option in the NAS Audio Output.



Note:

- Only the QNAP remote or MCE remote control is supported. NOT all the TS-x69 models support the internal remote control and the TS-x70 models only support the MCE remote control.
- Currently, the HDMI Audio Passthrough is not supported for the TS-x69 series.

Remote Control Mappings





	RM-IR001 Remote Control		Action	MCE Remote Control		XBMC Function	HD Station
Power	Power	1	N/A	Power	1	Power menu	
	Mute	2	OK	Mute	13	Mute	
Number	0,1,2,3,4,5,6,7,8,9	3	OK	0,1,2,3,4,5,6,7,8,9	18	0,1,2,3,4,5,6,7,8,9	
	Vol+, Vol-	4	OK	Vol+, Vol-	12	Vol+, Vol-	
	List/Icon	5	N/A			View mode	
	Search	6	N/A				

	TV Out	8	N/A				
	Settings	7	N/A			Settings	
Shortcut	Red - (Home)	9	OK	Red - (Home)	3	Home	
	Green (Video)	10	OK	Green (Video)	4	Video menu	
	Yellow (Music)	11	OK	Yellow (Music)	22	Music menu	
	Blue (Picture)	12	OK	Blue (Picture)	23	Photo menu	
Video Menu	Bookmark	13	N/A			Favorite	
	Repeater	14	N/A			Repeater	
	Guide	16	N/A			Help	
	Record	15	N/A				
	CH-	17	Previous	Previous	32	Skip back	
	CH+	18	Next	Next	33	Skip forward	
	Go to	20	N/A			Video progress bar	
	Info	19	OK	Info	10	File info	
Play Control	Home	21	OK			Home menu	
	Resume	22	N/A			Now playing	
	Return	28	OK	Back	7	Back	
	Options	29	N/A	More		Playback menu	
	OK	25	OK	OK	7	OK	OK
	Up	23	OK	Up	7	Up	Up
	Down	26	OK	Down	7	Down	Down
	Right	27	OK	Right	7	Right	Right

	Left	24	OK	Left	7	Left	Left
Video Play	Move backward	30	OK	Move backward	16	Move backward	
	Move forward	31	OK	Move forward	31	Move forward	
	Play	32	OK	Play	15	Play	
	Slow	33	N/A			Slow	
	Pause	34	OK	Pause	30	Pause	
	Stop	35	OK	Stop	33	Stop	
Video Setting	Audio	36	Audio List			Language track	
	Top/ Menu	37	Video List			Movie menu	
	Subtitle	38	OK	Subtitle	2	Subtitle track	
	Zoom	39	N/A			Zoom	
	Pop up	40	N/A			Movie menu	
	Angle	41	N/A			Angle	
Input				Clear (N/A)	19	Clear	
	OK			Enter	34	Confirm	
				Switch 16:9 / 4:3	27		

7.6 Download Station

The Download Station supports BT, HTTP, FTP, RapidShare, and Magnet download without a 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.

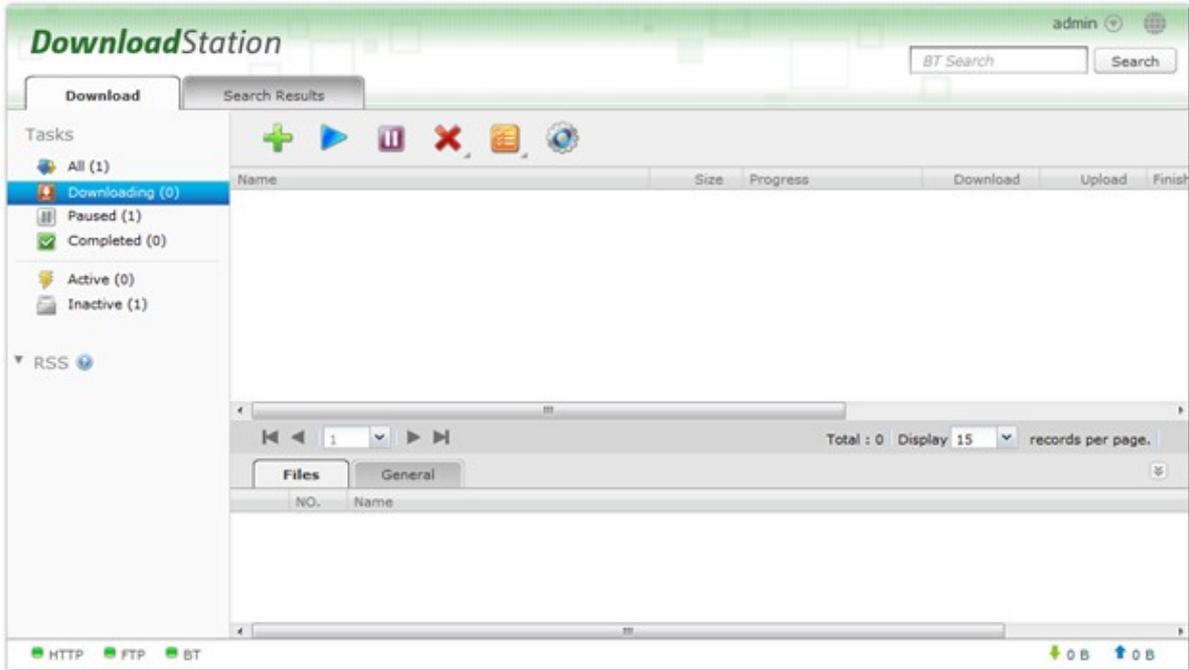
Go to "Administration" > "Applications" > "Download Station". Enable the service.



The screenshot shows a web interface for configuring the Download Station. The breadcrumb trail at the top reads "Home >> Applications >> Download Station". The main heading is "Download Station". Below this, there is a section titled "Download Station" containing a checked checkbox labeled "Enable Download Station". A note states: "After enabling this service, you may click the following link to enter the Download Station." Two links are provided: <http://10.8.13.59:8080/cgi-bin/Qdownload/qdownloadindex.cgi> and <https://10.8.13.59:443/cgi-bin/Qdownload/qdownloadindex.cgi>. An "APPLY" button is located in the bottom right corner of the configuration area.

Login the Download Station

Connect to the Download Station from the login portal of the NAS or click the service link on "Administration" > "Applications" > "Download Station".

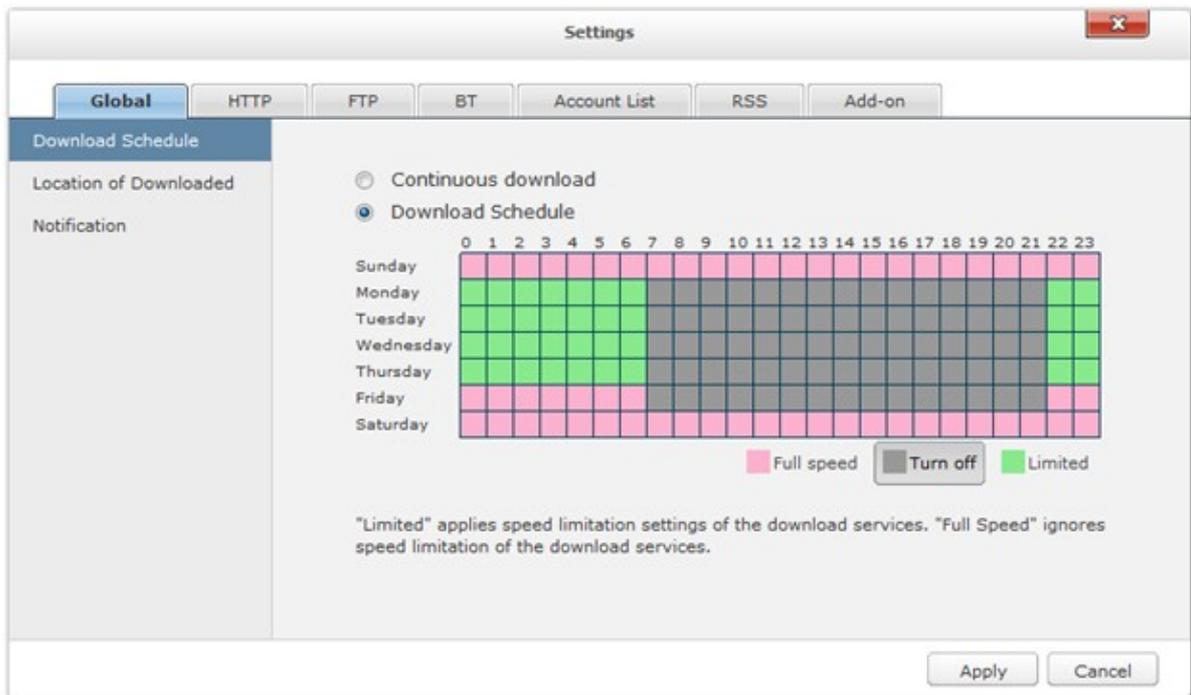


Before you start to download the files, click  to configure the settings.



Global Settings

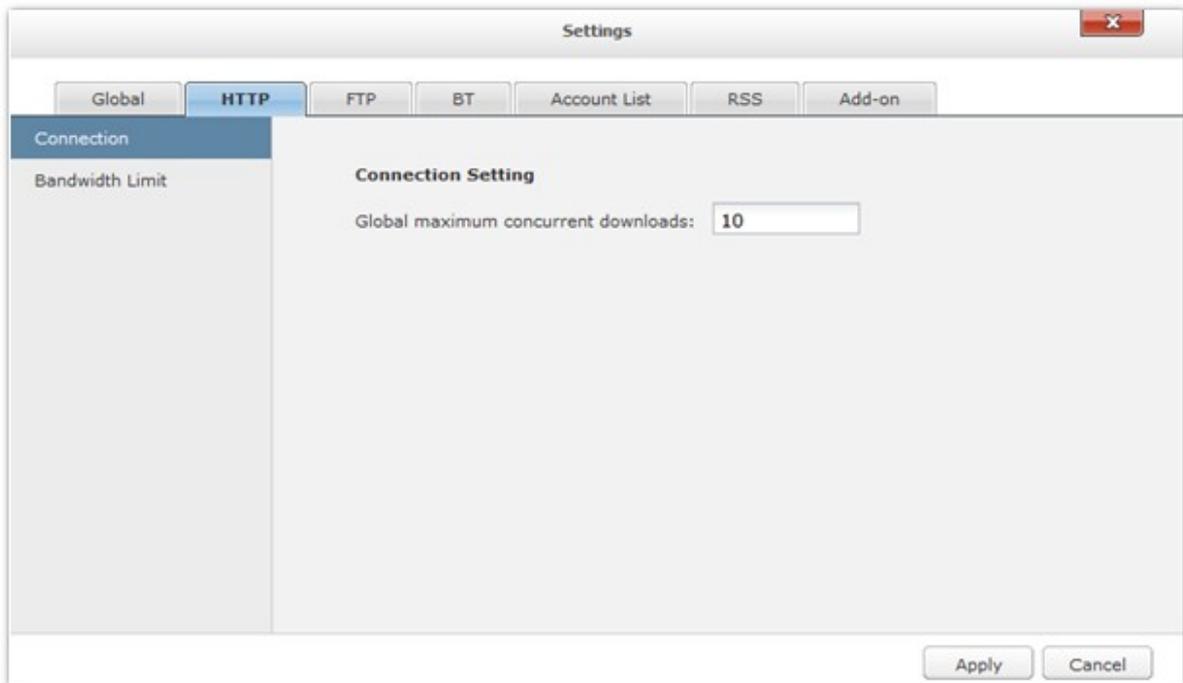
- Download Schedule: Select continuous download or specify the download schedule. When setting the download schedule, select "Full speed" to use the global speed limit (unlimited) for all the download tasks. Select "Limited" to apply the speed limit settings of the downloaded services.
- Location of Downloaded Files: Specify the default directory on the NAS for the downloaded files.
- Notification: Select to send a notification by email and/or instant messaging when a download task has completed. Note that the SMTP and IM settings must be configured properly in "System Administration" > "Notification".



HTTP

- Connection: Specify the maximum number of concurrent HTTP downloads.
- Bandwidth Limit: Specify the maximum download rate of HTTP download tasks. 0 means no limit.

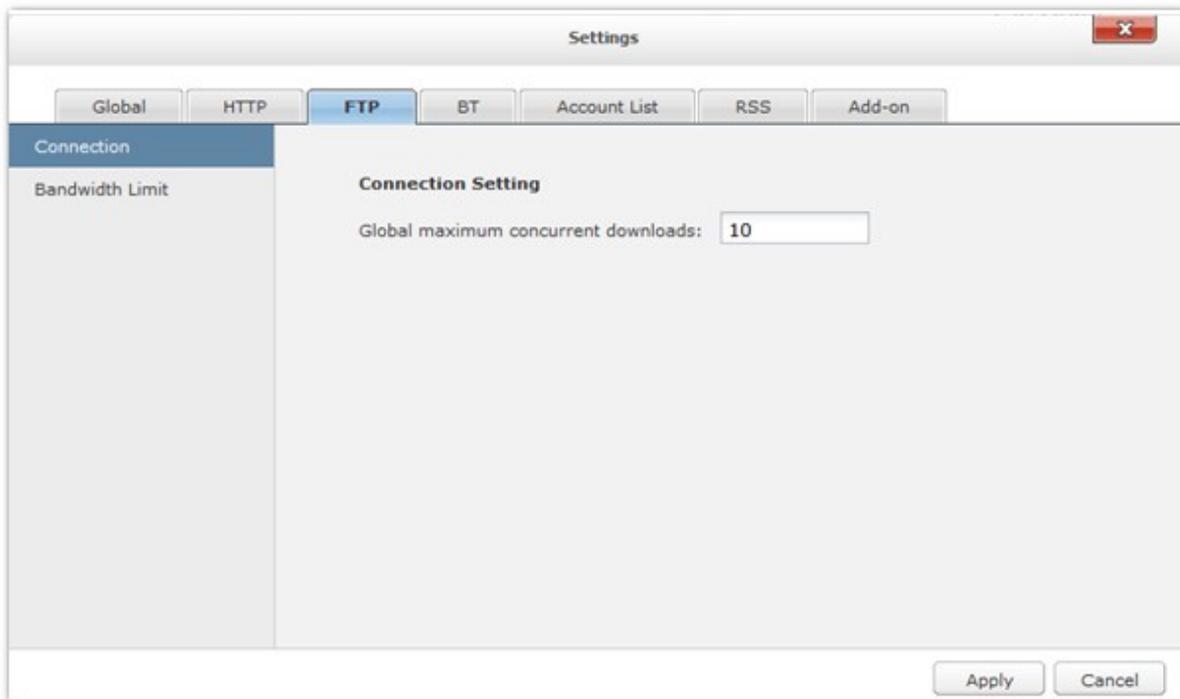
NAS models	Maximum number of concurrent downloads
Intel-based NAS	30
ARM-based (Non Intel-based) NAS	10



FTP

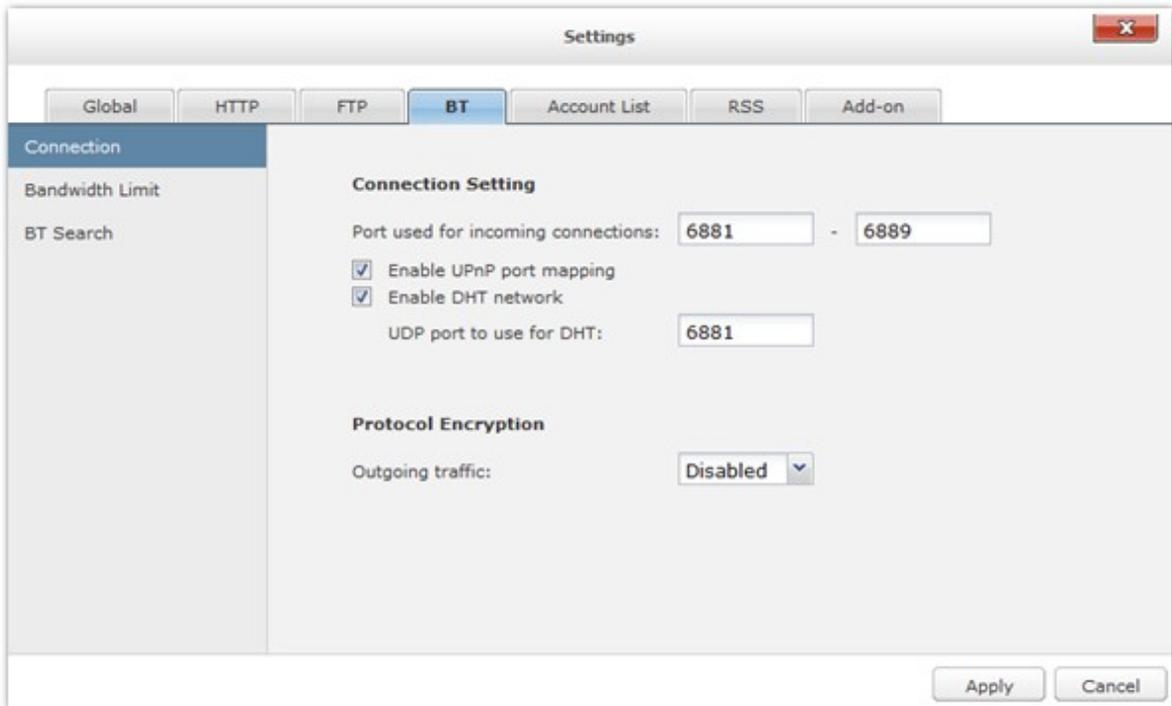
- Connection: Specify the maximum number of concurrent FTP downloads.
- Bandwidth Limit: Specify the maximum download rate of FTP download tasks. 0 means no limit.

NAS models	Maximum number of concurrent downloads
Intel-based NAS	30
ARM-based (Non Intel-based) NAS	10



BT

- Connection:
 - ✓ Specify the ports for BT download. The default port numbers are 6881-6889.
 - ✓ Enable UPnP port mapping: Enable automatic port mapping on the 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.
 - ✓ Protocol encryption: Enable this option for encrypted data transfer.



- Bandwidth Limit: Specify the maximum download rate of BT download tasks. 0 means no limit.

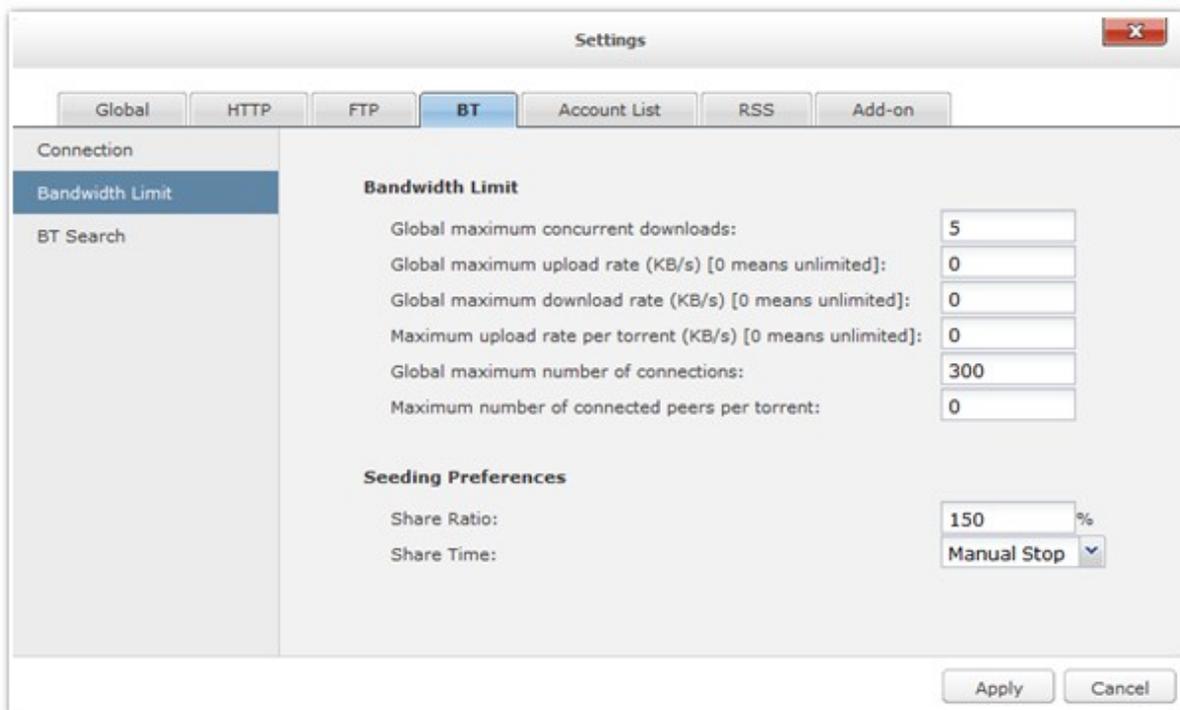
Global maximum concurrent downloads: Specify the maximum number of concurrent BT downloads.

NAS models	Maximum number of concurrent downloads
Intel-based NAS	30
ARM-based (Non Intel-based) NAS	10

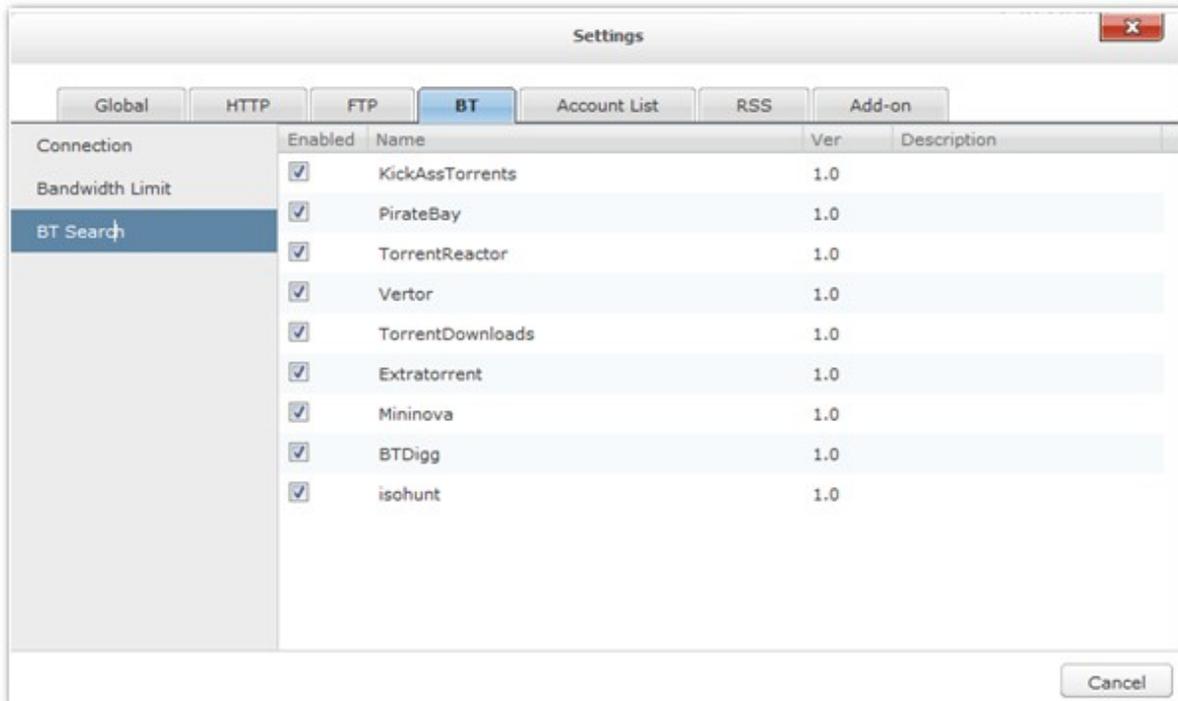
- ✓ Global maximum upload rate (KB/s): Enter the maximum upload rate for BT download. 0 means no limit.
- ✓ Global maximum download rate (KB/s): Enter the maximum download rate for BT download. 0 means no limit.
- ✓ Maximum upload rate per torrent (KB/s): Enter the maximum upload rate per torrent. 0 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.

Seeding Preferences:

Specify the share ratio for seeding a torrent and the sharing time. The share ratio is calculated by dividing the amount of uploaded data by the amount of downloaded data.

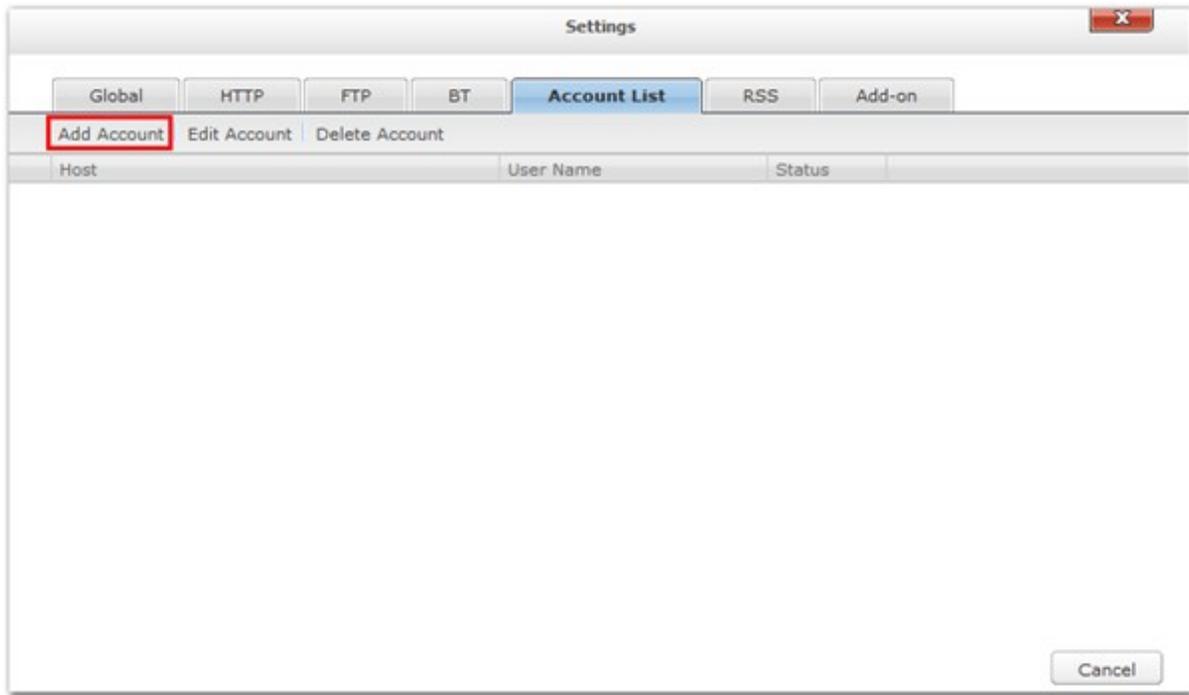


- BT Search: Select the BT engines to enable for BT search on the Download Station.



Account List

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".

Add a New Account:

Host: Input manually

Name:

Password:

Enabled:

Enter the host name or IP, username 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.

Add a New Account:

Host: Input manually

Name:

Password:

Enabled:

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".

Settings						
Global	HTTP	FTP	BT	Account List	RSS	Add-on
Add Account				Edit Account	Delete Account	
Host	User Name	Status				
rapidshare.com	qqq123	Enabled				
10.8.13.59	test	Enabled				

RSS

Update: Enable RSS download and specify the time interval to for the NAS to update the RSS feeds and check if any new contents that match the filters are available.

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".

Name	Last Check Date
------	-----------------

Filter Settings

Name:

Keyword:

Doesn't contain:

Feed:

Quality:

Episode Number: [ex. 1x12-14]

Check update every:

Save

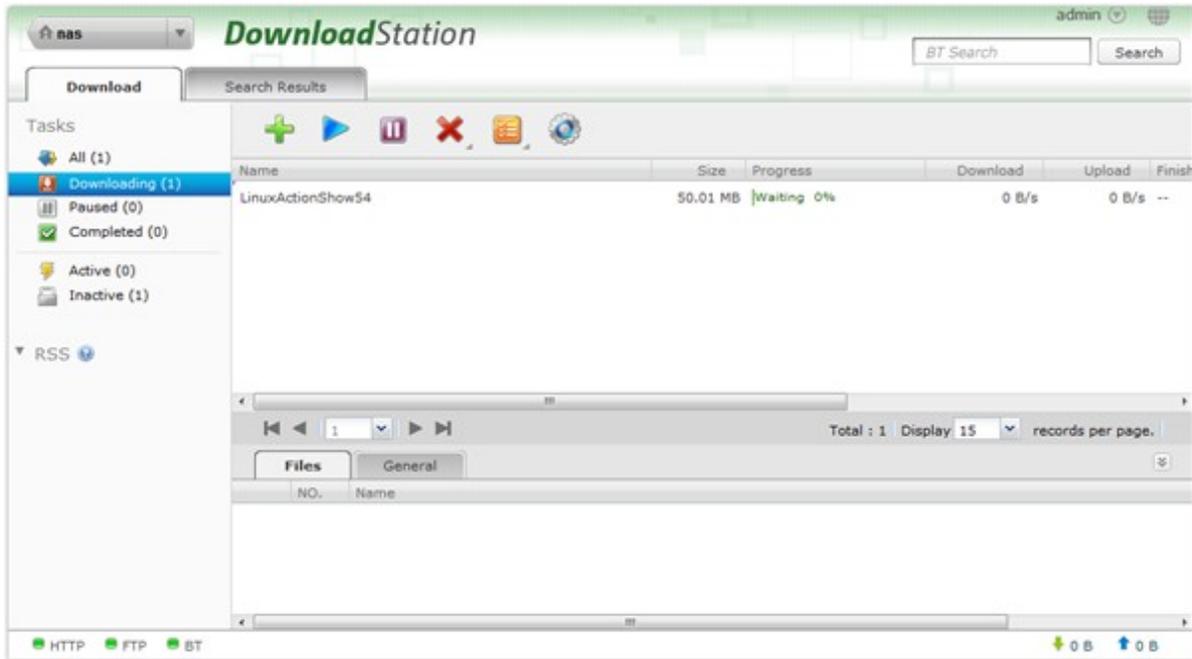
Cancel

Add-on

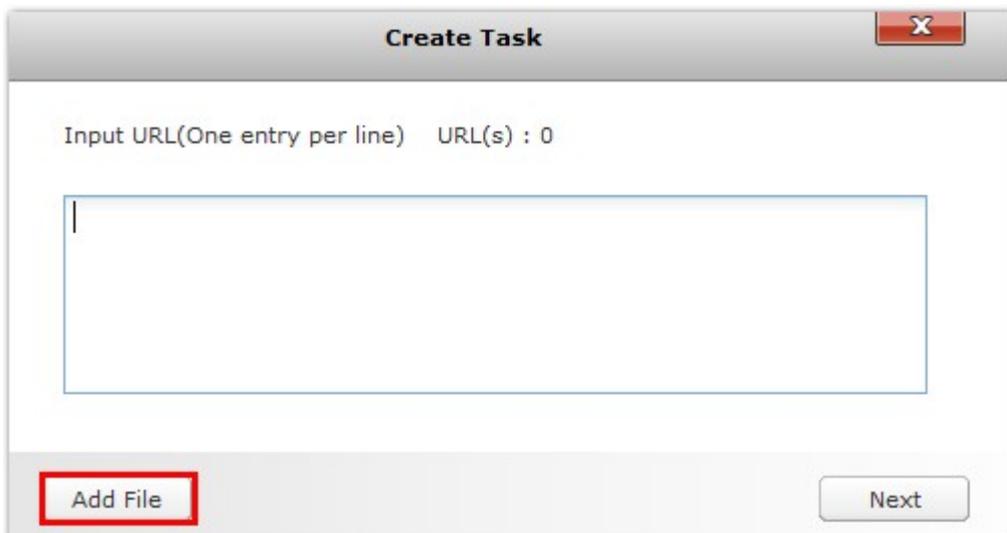
To download the YouTube videos by the HappyGet add-on to the NAS, enable the website subscription service. For more details, please see the application note: <http://www.qnap.com/en/index.php?sn=5319&lang=en>

BT Download

To download a BT file, click .



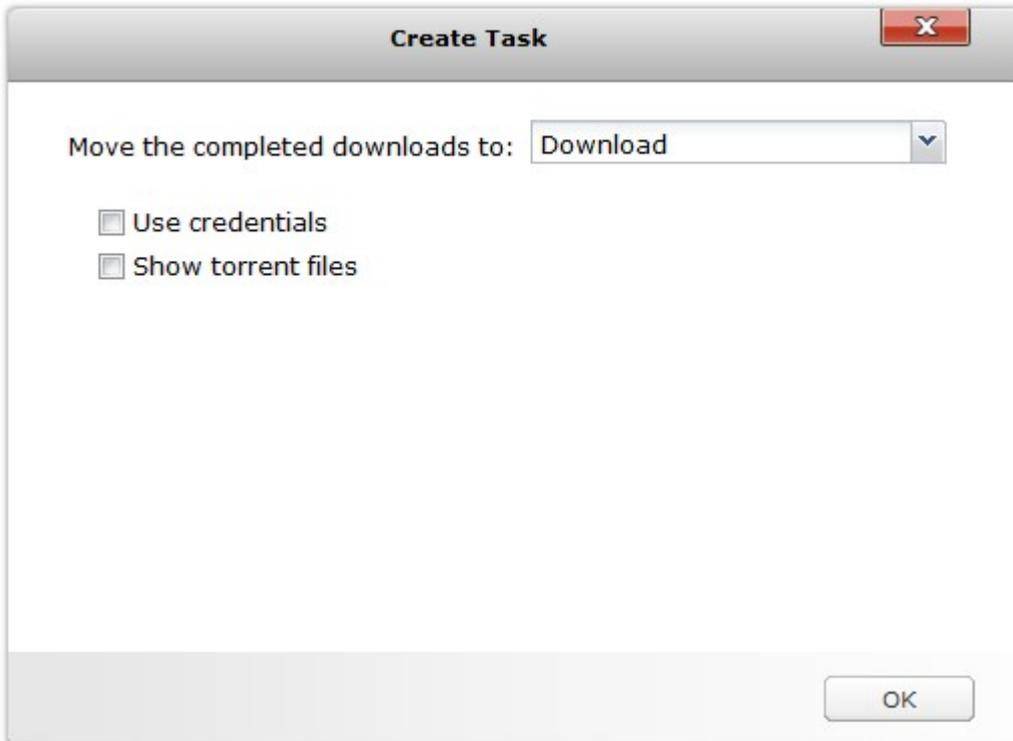
Click "Add File". Browse and select a torrent file.



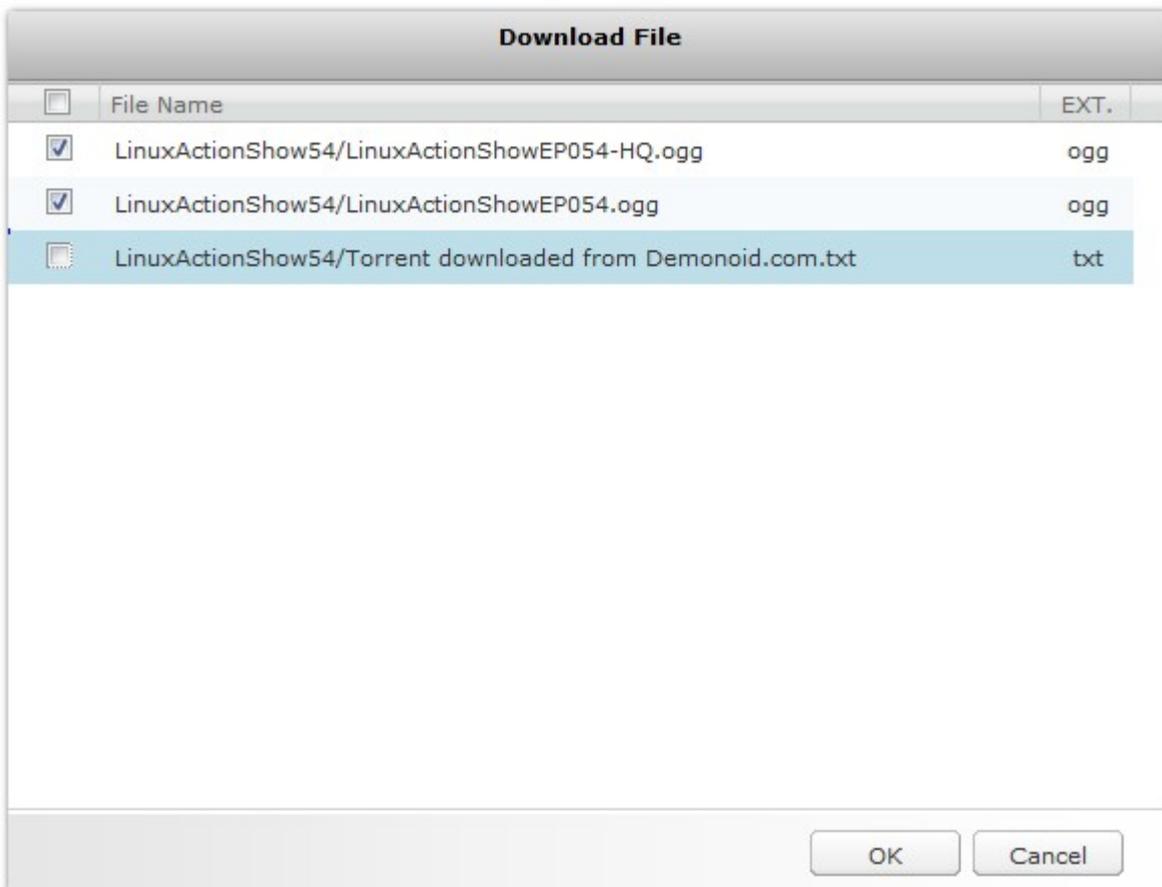
Specify the folder where the downloaded files will be saved to.

Use credentials: Select this option and enter the login information to download the files.

Show torrent files: Select this option to choose the files to download after clicking "OK".



Select the file(s) to download and click "OK".



Click the icons to manage the download tasks.

Icon	Description
	Start a download task.
	Pause a download task.
	Delete a download task.
	Start all, pause all, or pause all download tasks for a specified time period, remove all completed tasks, remove all completed tasks and delete data.

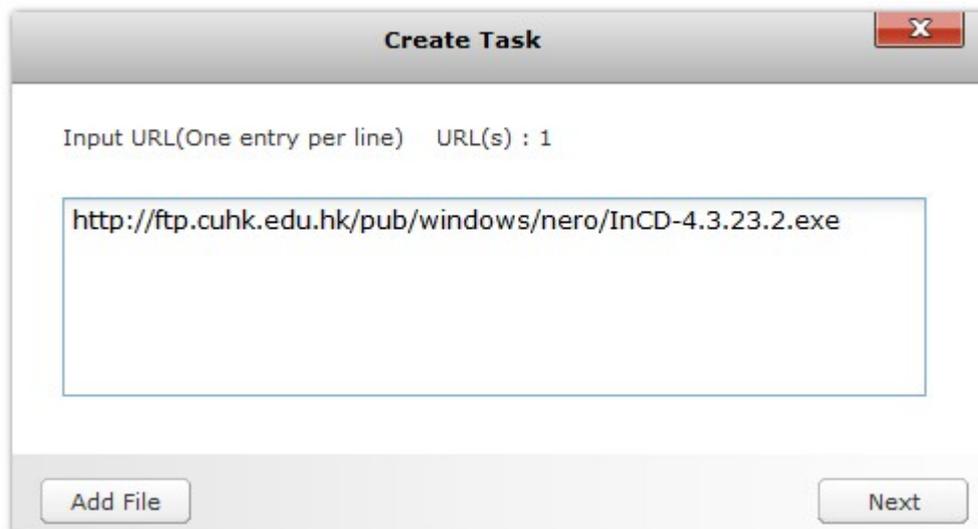
HTTP, FTP, RapidShare, Magnet Download

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 username and password is required to access the file, select "Use credentials" and select a pre-configured account (Settings > Account List) or enter a username and password. Then click "OK". The NAS will download the files automatically.

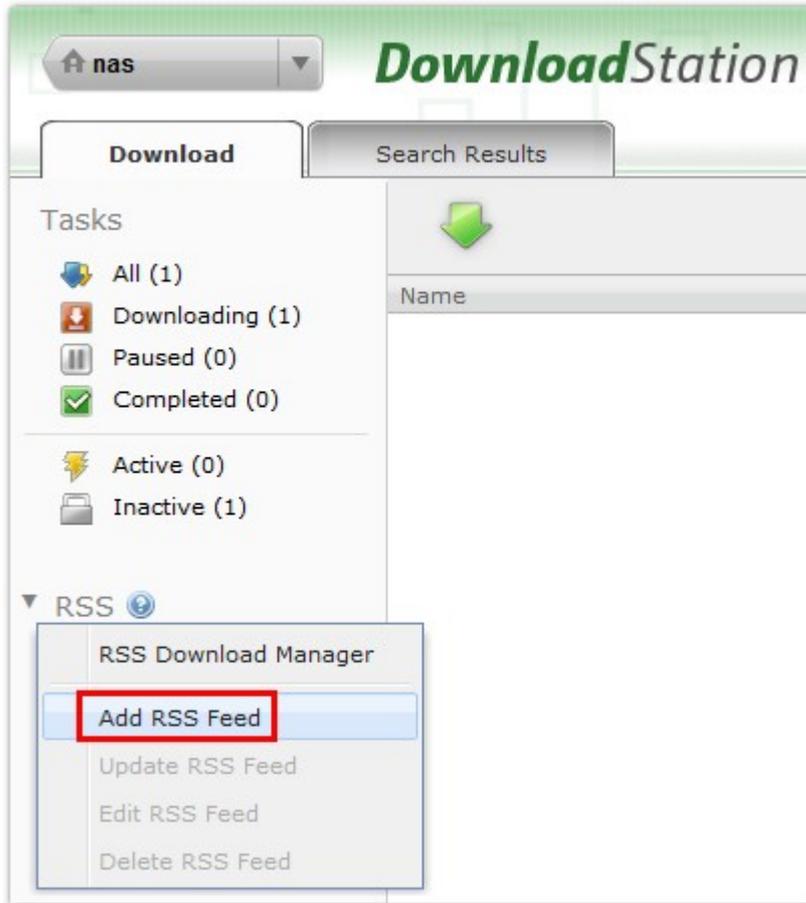
Note: You can only enter maximum 30 entries at one time.



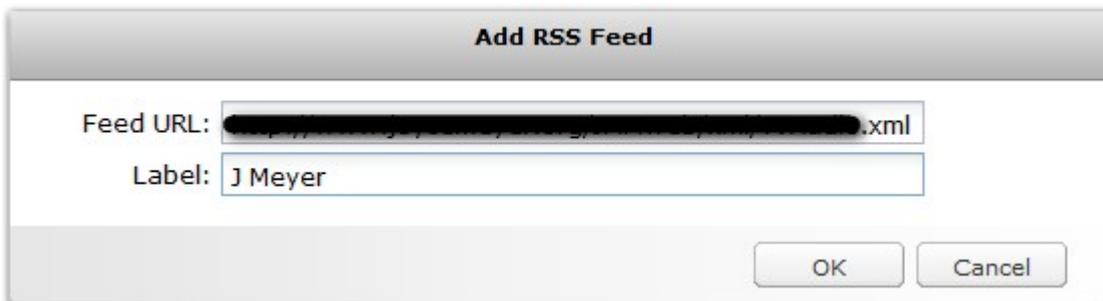
RSS Feed

You can subscribe to RSS feeds by the Download Station and download the torrent files in the feeds.

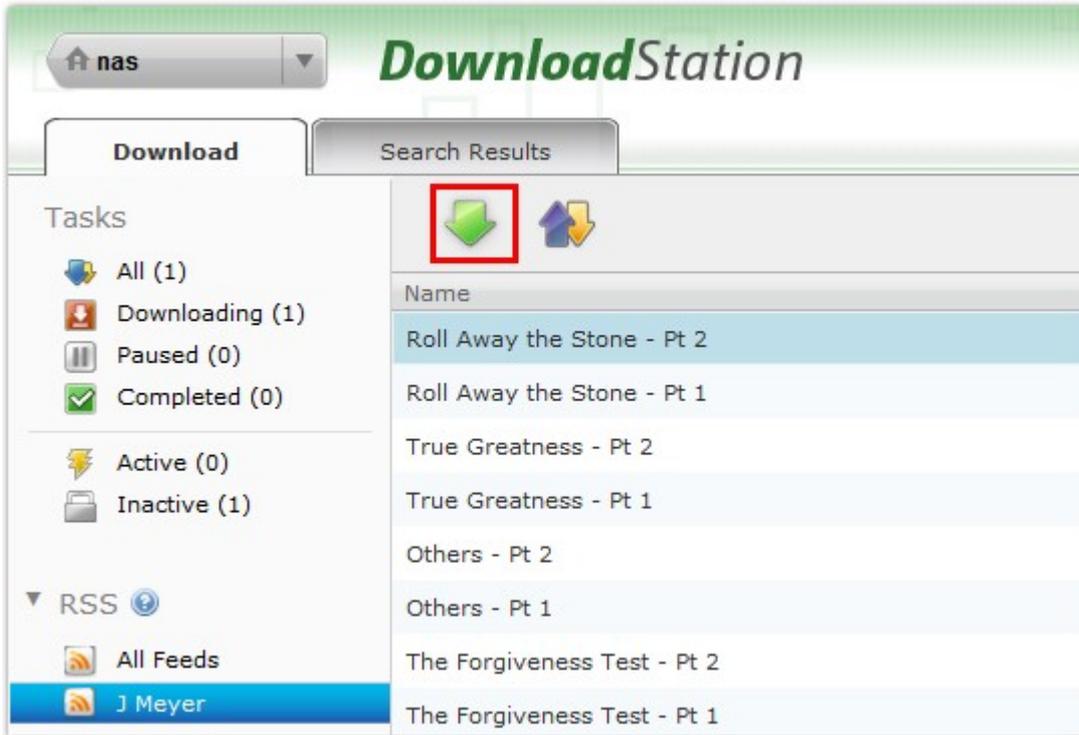
Click  to add an RSS feed.



Enter the URL and the label.

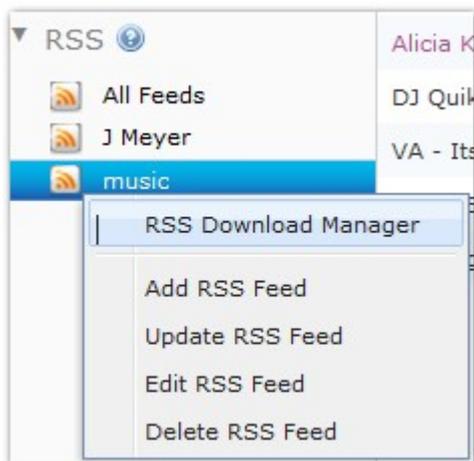


To download a torrent file from an RSS feed, select the file and click  or right click the feed and select "Download".



The NAS will start to download the file automatically. You can view the download status in the Downloading list.

To manage the RSS feeds subscription, right click an RSS feed label. You can open the RSS Download Manager, add, update, edit, or delete an RSS feed.



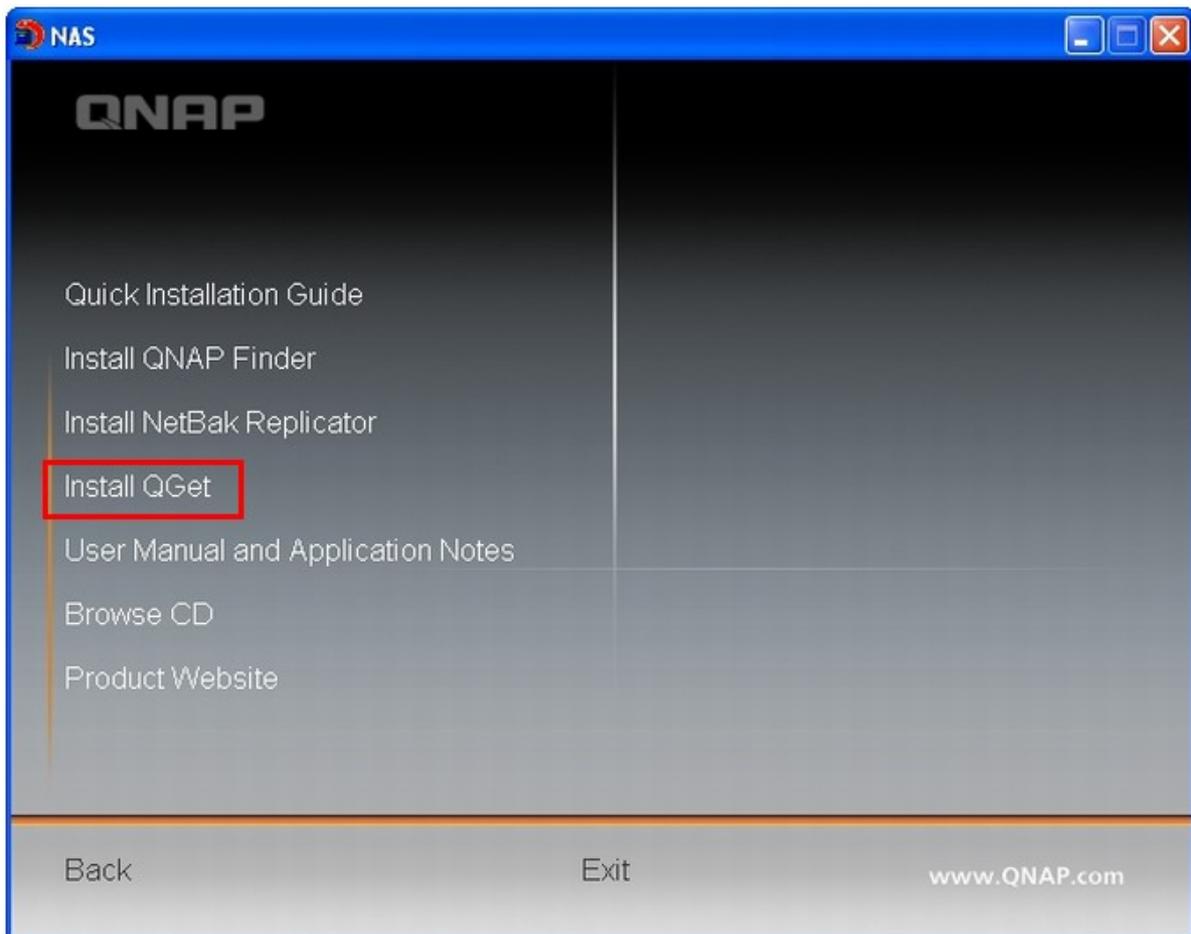
The common reasons for slow BT download rate or download error are as below:

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. Please download the latest version of QGet from <http://www.qnap.com/> to use with the Download Station 3.

1. Install QGet from the product CD-ROM disc.

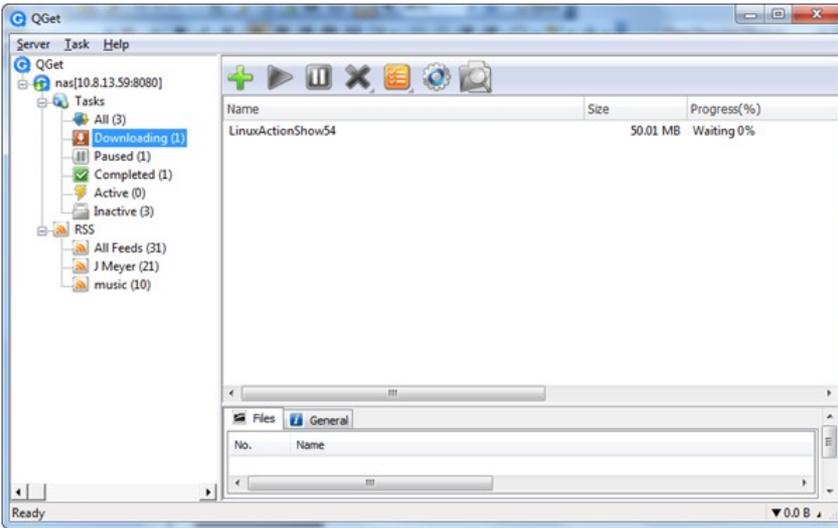


2. Follow the instructions to install QGet.



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".



7.7 Surveillance Station

The Surveillance Station offers live video monitoring and recording of IP cameras on the local network or the Internet. Enable this feature in "Administration" > "Applications" > "Surveillance Station".

The following Turbo NAS models support the Surveillance Station by default.

NAS models	Maximum number of supported IP cameras
TS-259 Pro+	2
TS-419U II, SS-439 Pro, TS-410U, TS-459 Pro+, TS-459 Pro II, TS-412U, SS-839 Pro, TS-859 Pro+, TS-879 Pro, TS-879U-RP, TS-EC879U-RP, TS-1079 Pro, TS-1279U-RP, TS-EC1279U-RP, TS-1679U-RP, TS-EC1679U-RP	4

Please visit <http://www.qnap.com/en/index.php?lang=en&sn=4056> for the IP cameras compatibility list.

Surveillance Station

Enable Surveillance Station

http://10.8.13.59:8080/cgi-bin/camera_view.cgi

Note: The Surveillance Station only supports 32-bit Internet Explorer version 7.0 or above.

Download Surveillance Station Pro

You can download Surveillance Station Pro for Installation.

Surveillance Station Pro supports more cam models, and equipped with multiple monitoring, advanced alarm settings, intelligent playback features. You can also perform remote management by Vmobile on iOS or Android devices. Click [HERE](#) to download Surveillance Station Pro.

Note: The Surveillance Station Pro offers one free recording channel. To add extra number of recording channels, please purchase the license at QNAP License Store (<http://license.qnap.com>) or contact an authorized reseller for assistance.

APPLY

About Surveillance Station Pro

The Surveillance Station Pro is an advanced version of the Surveillance Station. The application is compatible with more than 1400 IP cameras, supports adding extra number of recording channels by license management, user access control, advanced alarm settings, etc. The Surveillance Station Pro offers **one** free recording channel by default. To add extra number of recording channels, please purchase the license at the QNAP License Store (<http://license.qnap.com>) or contact an authorized reseller.

The following Turbo NAS models support the Surveillance Station Pro by default.

NAS models	Maximum number of supported IP cameras (free)
TS-469 Pro, TS-569 Pro, TS-669 Pro, TS-869 Pro, TS-269 Pro, TS-469U-RP, TS-869U-RP, TS-269L, TS-469L, TS-569L, TS-669L, TS-869L, TS-469U-SP	1

The Surveillance Station Pro can be installed on other Turbo NAS models by installing the add-on in "Applications" > "QPKG Center".

NAS models	Maximum number of recording channels supported (by license purchase with the Surveillance Station Pro)
ARM series (TS-x10, x12, x19)	8
x86 series (TS-x39, x59, x69)	16
TS-x79 series	40

Use the Surveillance Station

Click the service link on "Administration" > "Applications" > "Surveillance Station" to connect to the application. Enter the username and password when you are prompted to.

Note: The Surveillance Station only supports 32-bit Internet Explorer version 7.0 or above.

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)

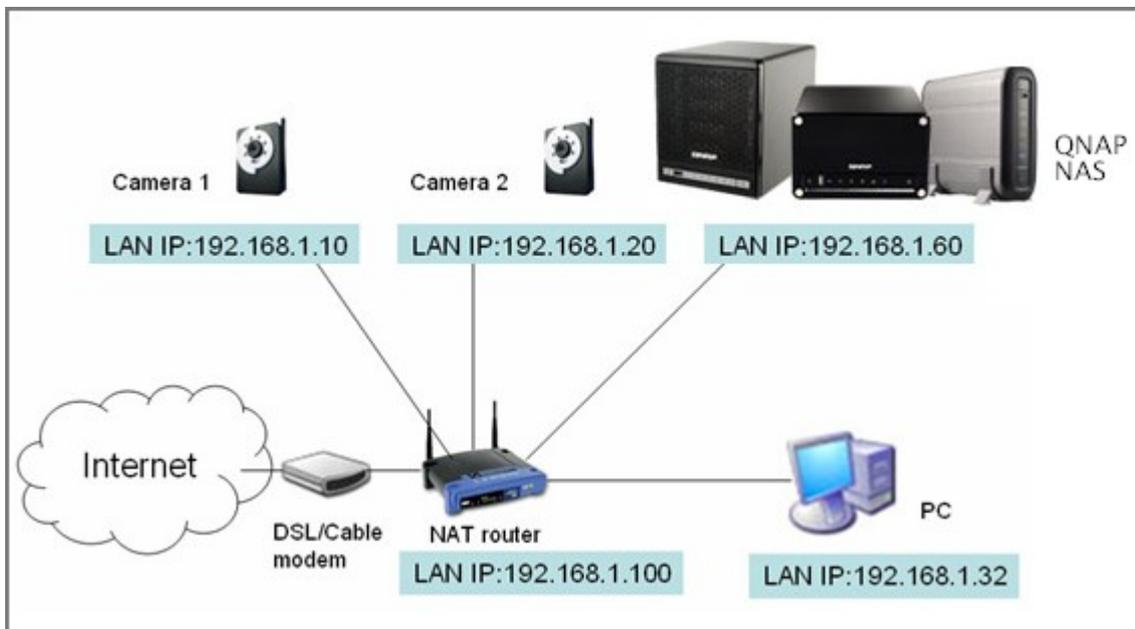
Plan your home network topology

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.

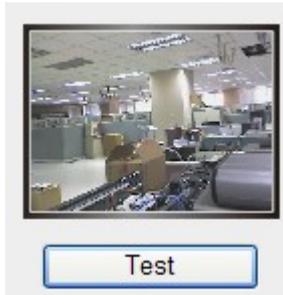
The screenshot shows the 'Surveillance Station' interface for a Network Video Recorder. The 'Settings' tab is active, and the 'Camera Settings' sub-tab is selected. A table lists two cameras: 'Camera 1' and 'Camera 2'. Below the table, the configuration for 'Camera 1' is shown. Fields include: Camera Number (1), Camera Model (Axis 205), Camera Name (Camera 1), IP Address (empty), Port (80), WAN IP (empty), and User Name/Password (empty). A 'Test' button is next to a video preview window. 'Apply' and 'Remove' buttons are at the bottom.

	Camera Name	Brand	IP Address	WAN IP Address
1	Camera 1			
2	Camera 2			

Camera Number: 1: Camera 1
Camera Model: Axis 205
Camera Name: Camera 1
IP Address:
 Port: 80
WAN IP: (for monitoring from public network)
(If your IP camera is installed behind NAT router, you may input the public IP address (or URL) and the corresponding forwarded port of the router.)
 Port: 80
User Name:
Password:
[Apply] [Remove]

Note: All the camera configuration will not take effect until you click the "Apply" button.

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



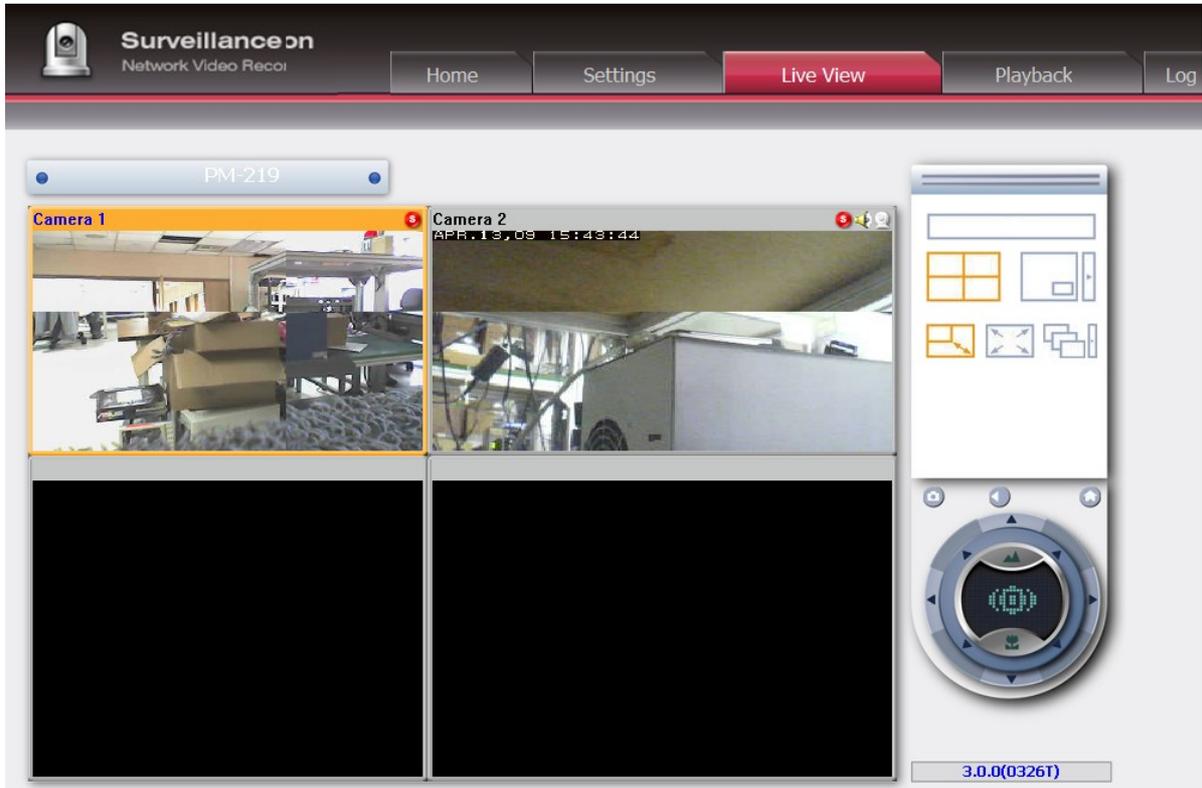
If your IP camera supports audio recording, you may enable the option on the "Recording Settings" page. Click "Apply" to save the changes.

Camera Number:	2: Camera 2	▼
Video Compression:	Motion JPEG	▼
Resolution:	QVGA	▼
Frame Rate:	20	▼
Quality:	Normal	▼
<input checked="" type="checkbox"/> Enable audio recording on this camera		
Estimated Storage Space for Recording: 6760 GB		
<input type="button" value="Apply"/>		

Configure the settings of IP camera 2 following the above steps.

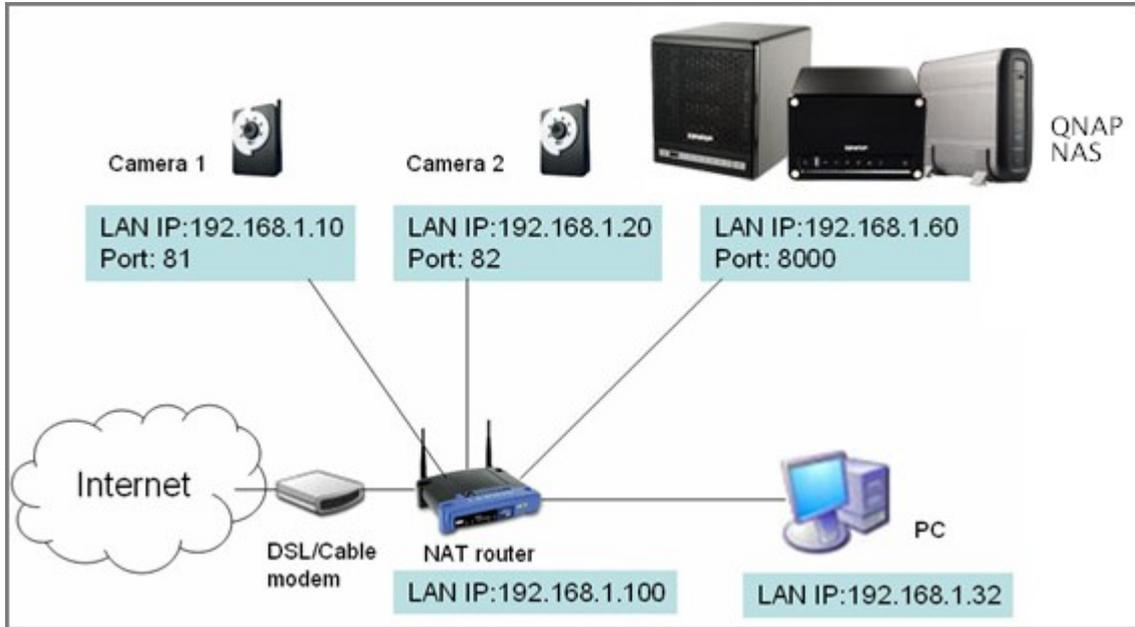
After you have added the network cameras to the NAS, go to the "Live View" page. The first time you connect to this page by the IE browser, you have to install the ActiveX control in order to view the images of IP camera 1 and IP camera 2. You can start to use the monitoring and recording functions of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

Camera Number:	1: Camera 1	
Camera Model:	iPUX ICS 1003/1013	
Camera Name:	Camera 1	
IP Address:	192.168.1.10	
<input checked="" type="checkbox"/> Port	81	
WAN IP: (for monitoring from public network)	myNAS.dyndns.org	
<small>(If your IP camera is installed behind NAT router, you may input the public IP address (or URL) and the corresponding forwarded port of the router.)</small>		
<input checked="" type="checkbox"/> Port	81	
User Name :	administrator	
Password :	•••••	
<input type="button" value="Apply"/> <input type="button" value="Remove"/>		<input type="button" value="Test"/>

Note: All the camera configuration will not take effect until you click the "Apply" button.

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

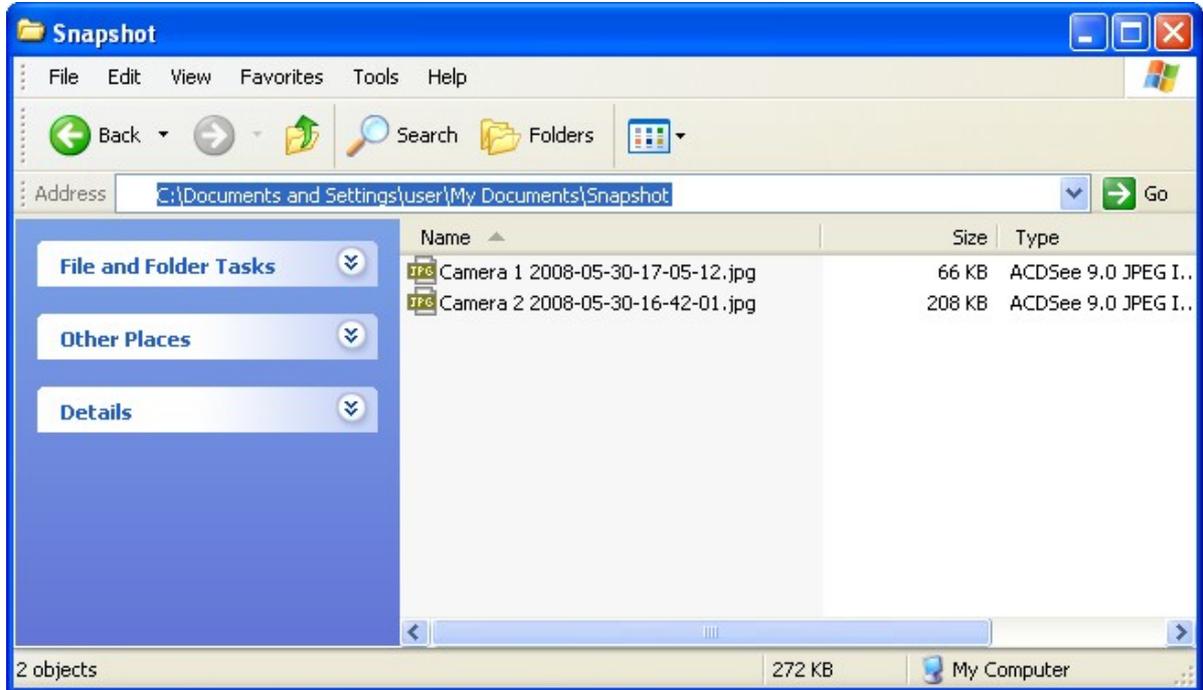
- Forward port 8000 to the LAN IP of the NAS: 192.168.1.60
- Forward port 81 to the LAN IP of IP camera 1: 192.168.1.10
- Forward port 82 to the LAN IP of IP camera 2: 192.168.1.20

Note: When you change the port settings, make sure remote access is allowed. For example, if your 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".

7.8 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.

iTunes Server

iTunes Server

After enabling iTunes server, all the iTunes clients on the same subnet can play the music files in "Multimedia" folder on the server.

Enable iTunes Server

After enabling this service, click the following link to enter iTunes Web Server configuration page.

<http://10.8.12.95:3689/index.html>

User Name: admin

Password:

To configure the iTunes server settings and add smart playlists, login the web page of iTunes server:
<http://NAS-IP:3689/index.html>

The screenshot shows the Firefly web interface. At the top left is the Firefly logo and the text "The best open-source media server for the Roku SoundBridge and iTunes". Below this is a navigation menu with links: "server status", "smart playlists", "configuration", "about firefly", "thanks", and "Version svn-1696". The main content area is titled "Configuration" and includes a "Show advanced config" link. The configuration is divided into three sections: "Server", "Music Files", and "Database".

Server

Config File Location	/mnt/HDA_ROOT/.config/mt-daapd.conf	
Server Name	<input type="text" value="KenTest659(iTunes)"/>	The name iTunes and other daap clients should see
Logfile	<input type="text"/>	
Admin password	<input type="text" value="admin"/>	The password for this administration interface.
Music Password	<input type="text"/>	The password clients need to access this server.

Music Files

Music Folder	<input type="text" value="/share/Multimedia"/>
Remove	
Music Folder	<input type="text" value="/share/Public"/>
Remove	
	Add music folder
Extensions	<input type="text" value=".mp3,.m4a,.m4p,.aif,.wav,."/>
Playlist File	<input type="text"/>

Database

Scan Type	<input type="text" value="0 - Normal"/>	
Rescan Interval	<input type="text" value="180"/>	How often should Firefly look for new files? In seconds.
Always Scan	<input type="text" value="No"/>	

At the bottom of the configuration area are "Save" and "Cancel" buttons.

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.



7.9 DLNA Media Server

To allow DLNA media players to access and play the multimedia contents on the NAS, enable this feature and click the link (<http://NAS IP:9000/>) to enter the configuration page of the DLNA 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 DLNA media server of the NAS for media playing, see here [700](#).

7.10 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](#).

MySQL Server

MySQL Server

You can enable MySQL server as the website database.

Enable MySQL Server
Enable this option to allow remote connection of MySQL server.

Enable TCP/IP Networking
Port Number:

Note: You can install the phpMyAdmin package to manage your MySQL server. To install the phpMyAdmin, please click [here](#).

Database Maintenance

You can reset the database password or re-initialize the database.

7.11 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.

QPKG Center

INSTALLED **AVAILABLE** **GET MORE**

Category: **ALL** ▼

	AjaXplorer 2.5.5 QNAP Systems, Inc.	AjaXplorer is a file explorer for remotely managing files on a web server or operation as a simple file-sharing system. Its rich layout	» Installed Forum · Wiki [More]
	Asterisk 1.4.22.1b Adnovea	Asterisk is a software implementation of a PBX that allows attached telephones to make calls to one another, and to connect to other telephone services including the PSTN and VoIP services. Requires the Optware QPKG.	» Install » Download Forum · Wiki
	eyeOS 1.9.0.1 Christopher	eyeOS is an open source web desktop following the cloud computing concept that leverages collaboration and communication among users.	» Install » Download Forum · Wiki [More]

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).

QPKG Center

INSTALLED **AVAILABLE** **GET MORE**

CHECK FOR UPDATE

	Airplay 0.18_b1 Cristian && ADoko	No Description Available	» Enable » Remove
	AirVideoServer Alpha.6-r6 Cristian	No Description Available Web Page: http://10.8.12.95:80/avs https://10.8.12.95:8081/avs	» Enable » Remove
	AjaXplorer 2.5.5 Based on the original work of Charles du Jeu	AjaXplorer is a file explorer for remotely managing files on a web server or operation as a simple file-sharing system. Its rich layout	» Remove [More] Web Page: http://10.8.12.95:80/AjaXplorer/ https://10.8.12.95:8081/AjaXplorer/

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".



7.12 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.

Syslog Server Configuration

SERVER SETTINGS **FILTER SETTINGS** **SYSLOG VIEWER**

Server Settings

Enable Syslog Server

Enable TCP

 TCP Port:

Enable UDP

 UDP Port:

Log Settings

Maximum Log Size (MB):

Log File: /

Email Notification

If the severity of a received log message is higher the selected severity level, the system will send an alert email automatically.

Enable the email notification

 Severity level:

Note: The SMTP server must be configured first for alert mail delivery. [Click this to configure the SMTP server](#)

APPLY

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 "Applications" > "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.

Email Notification

If the severity of a received log message is higher the selected severity level, the system will send an alert email automatically.

Enable the email notification

Severity level: ▼

Note: The SMTP server must be configured first for alert mail delivery. [Click this to configure the SMTP server](#)

APPLY

Filter Settings

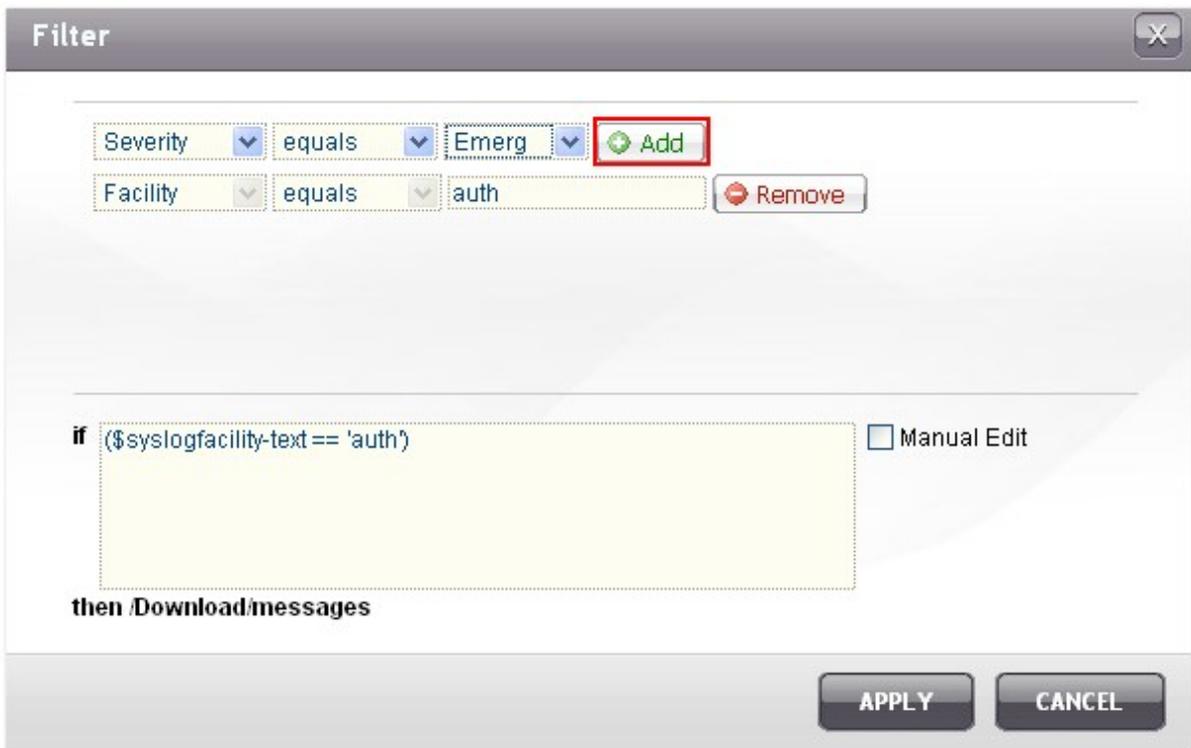
This feature should only be operated by system administrators who are familiar with syslog filters.

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



The screenshot shows the 'Syslog Server Configuration' interface. It has three tabs: 'SERVER SETTINGS', 'FILTER SETTINGS' (which is active), and 'SYSLOG VIEWER'. In the top right corner, there is a button labeled 'Add a New Filter'. Below this is a table with the following columns: a checkbox, 'Filter', 'Status', and 'Action'.

<input type="checkbox"/>	Filter	Status	Action
<input type="checkbox"/>	(\$syslogfacility-text == 'auth')	Disable	 
<input type="checkbox"/>	(\$syslogfacility-text == 'auth') and (\$syslogseverity-text == 'emerg')	Enable	 

At the bottom left of the table area, there is a 'Delete' button with a red arrow icon.

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".

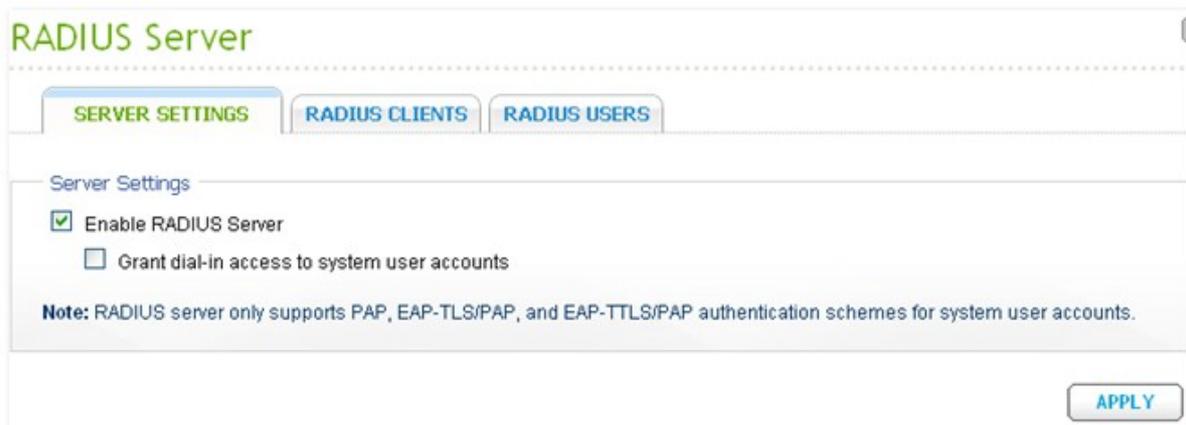
SERVER SETTINGS FILTER SETTINGS SYSLOG VIEWER								
Latest Log ▾								
Date	Time	Facility	Severity	Hostname	Application	P.ID	M.ID	Message
2011-09-14	16:41:11 +08:00	auth	Info	nas	qlogd	5830	-	qlogd[5830]: conn log: Users: admin, Source IP: 10.8.12.38, Computer name: ---, Connection type: HTTP, Accessed 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

7.13 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".



The screenshot shows the "RADIUS Server" configuration page with the "SERVER SETTINGS" tab selected. The "Enable RADIUS Server" checkbox is checked, and the "Grant dial-in access to system user accounts" checkbox is unchecked. A note states: "Note: RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication schemes for system user accounts." An "APPLY" button is located at the bottom right.

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".



The screenshot shows the "RADIUS Server" configuration page with the "RADIUS CLIENTS" tab selected. A "Create a New Client" button is highlighted with a red box. Below the button is a table with columns: Name, IP Address, Prefix Length, Status, and Action. A "Delete" button is located at the bottom left.

	Name	IP Address	Prefix Length	Status	Action
<input type="checkbox"/>					

b. Enter the client information and click "Apply".

RADIUS Clients

QNAP
TURBO NAS

Create a New Client

Name:

IP Address:

Prefix Length:

Secret Key:

APPLY **CANCEL**

c. The clients are shown on the list.

RADIUS Server

SERVER SETTINGS **RADIUS CLIENTS** **RADIUS USERS**

[Create a New Client](#)

<input type="checkbox"/>	Name	IP Address	Prefix Length	Status	Action
<input type="checkbox"/>	WirelessAP1	192.168.1.0	24	Enabled	
<input type="checkbox"/>	WirelessAP2	192.168.2.0	24	Enabled	
<input type="checkbox"/>	WirelessAP3	10.0.1.0	24	Enabled	

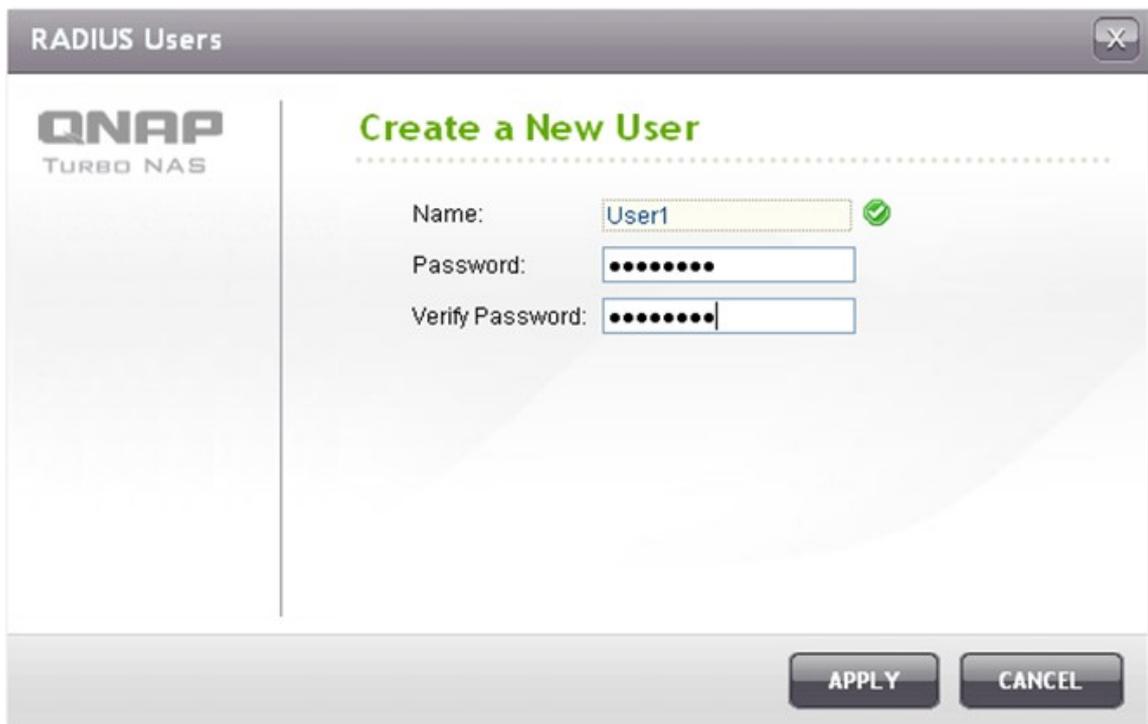
Delete

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.

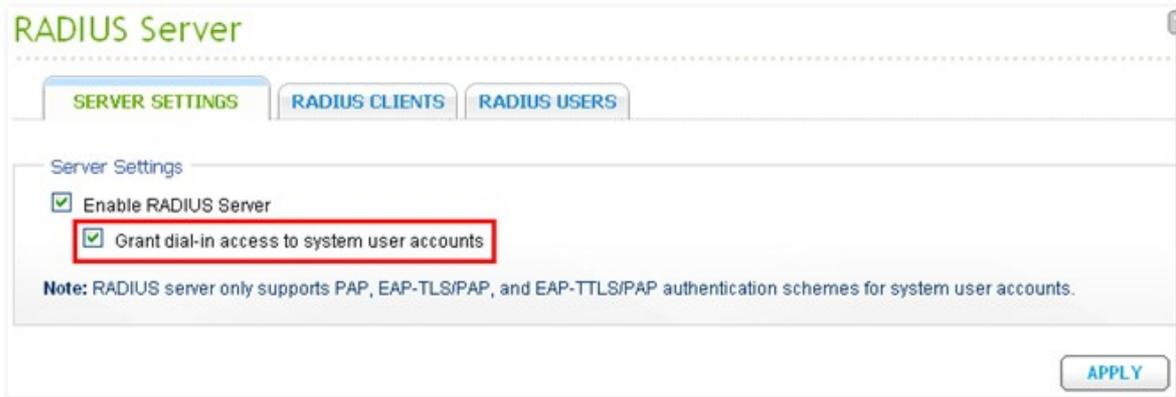
- a. Click "Create a New User".



- b. Enter the username and password. The username 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".



- 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".



The screenshot shows the 'RADIUS Server' configuration window. At the top, there are three tabs: 'SERVER SETTINGS' (selected), 'RADIUS CLIENTS', and 'RADIUS USERS'. Under the 'SERVER SETTINGS' tab, there is a section titled 'Server Settings'. It contains two checked checkboxes: 'Enable RADIUS Server' and 'Grant dial-in access to system user accounts'. The second checkbox is highlighted with a red rectangular border. Below the checkboxes, there is a note: 'Note: RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication schemes for system user accounts.' At the bottom right of the window, there is an 'APPLY' button.

Note: The RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication for local NAS user accounts.

7.14 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 username and password to authenticate the Rsync server which attempts to back up data to the NAS.

Backup Server

RSYNC SERVER | **RTRR SERVER**

Rsync Server Settings

By using this function, you can back up the data on the local server to a remote server of the same NAS series, and also allow backup from remote server to the local server.

Port Number:

Maximum download rate (KB/s):

Enable backup from a remote server to the local host

Allow remote Rsync server to back up data to NAS

User Name:

Password:

APPLY

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.

RSYNC SERVER **RTRR SERVER**

RTRR Server Settings

Real-time Remote Replication (RTRR) Server allows you to perform one-way synchronization from the local NAS to a remote server, or other way round.

Enable Real-time Remote Replication Server

Port Number:

Maximum upload rate (KB/s):

Maximum download rate (KB/s):

Password

Password:

Verify Password:

Network Access Protection

Allow all connections

Allow connections from the list only

<input type="checkbox"/>	Genre	IP address or network domain	Access right	Action
<input type="button" value="Delete"/>				

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".

Network Access Protection

Allow all connections
 Allow connections from the list only

<input type="checkbox"/>	Genre	IP address or network domain	Access right	Action
<input type="button" value="Delete"/>				

Note: If the list is empty, all connections to the server will be allowed.

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.

Add IP Address

QNAP TURBO NAS

Enter the IP addresses that are allowed to connect to the server.

IP Address Format: IPv4

Single IP address
 Specify IP addresses of certain network by setting IP address and netmask

IP Address: [] . [] . [] . []

IP: 10 . 8 . 0 . 0

Subnet Mask: 255 . 0 . 0 . 0

Access right: Read/Write

Step 1 of 1

After saving the access rule, click "Apply" and the NAS will restart to apply the settings.

Network Access Protection

Allow all connections

Allow connections from the list only

<input type="checkbox"/>	Genre	IP address or network domain	Access right	Action
<input type="checkbox"/>	LAN2	10.8.0.0/8	Read/Write	

Note: If the list is empty, all connections to the server will be allowed.

Note: The settings have been changed. Please click "Apply" to restart the server.

7.15 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 "Applications" > "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:

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.

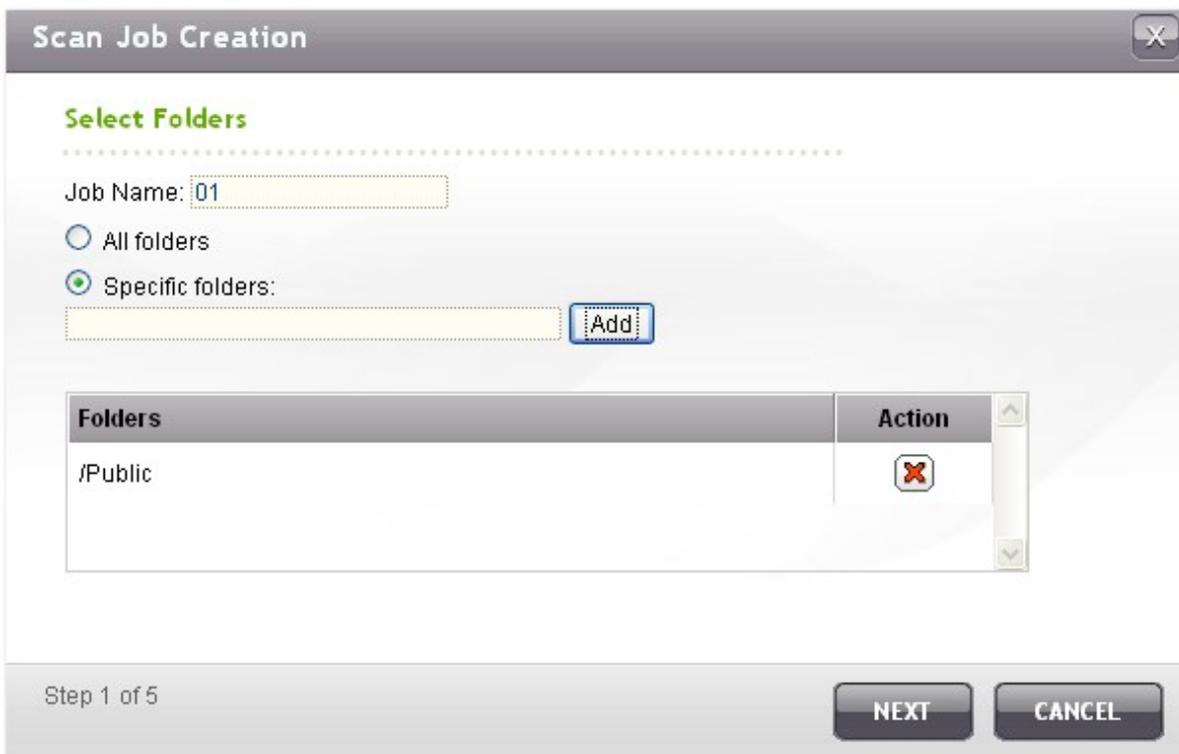
1. Go to "Applications" > "Antivirus" > "Scan Jobs". Click "New Scan Job".



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".



Scan Job Creation

Select Folders

Job Name:

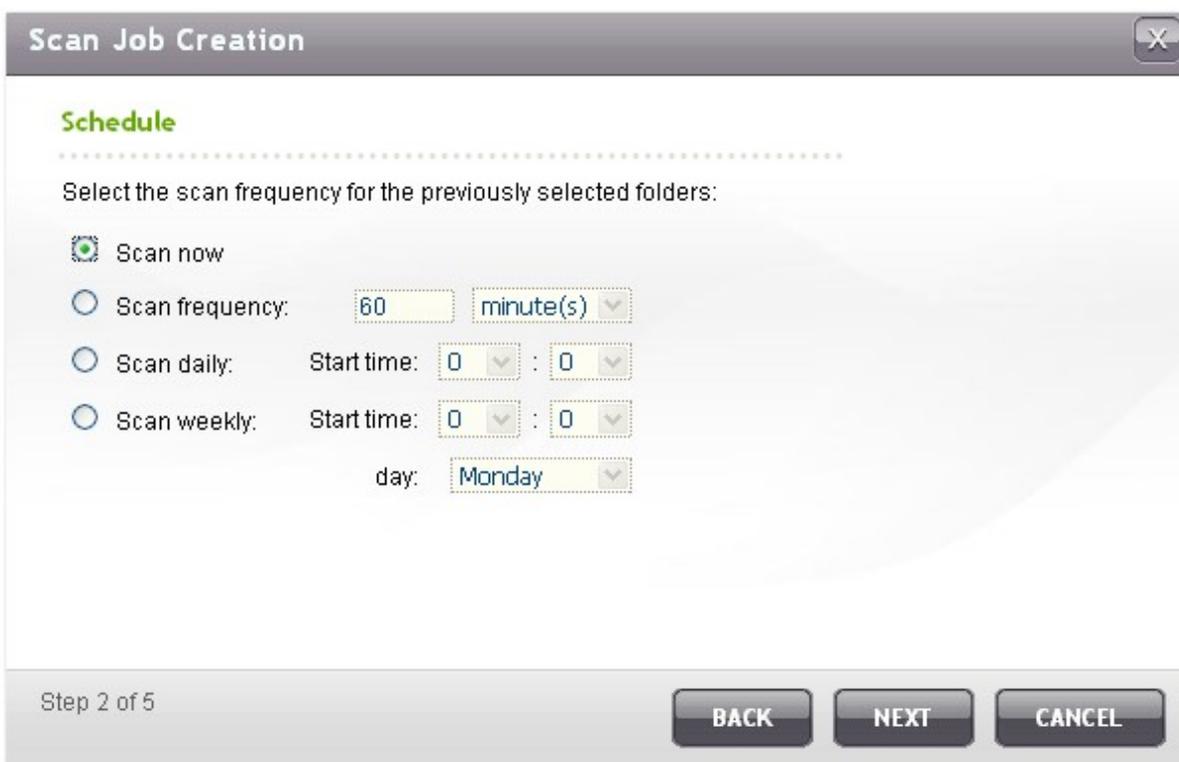
All folders

Specific folders:

Folders	Action
/Public	

Step 1 of 5

4. Define the schedule for the scan job. Click "Next".



Scan Job Creation

Schedule

Select the scan frequency for the previously selected folders:

Scan now

Scan frequency:

Scan daily: Start time: :

Scan weekly: Start time: :
day:

Step 2 of 5

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".

Scan Job Creation [X]

Scan Options

Maximum file size for scanning (MB) 25

Scan compressed files

Maximum amount of data in an archive file for scanning (MB) 100

Scan documents ⓘ

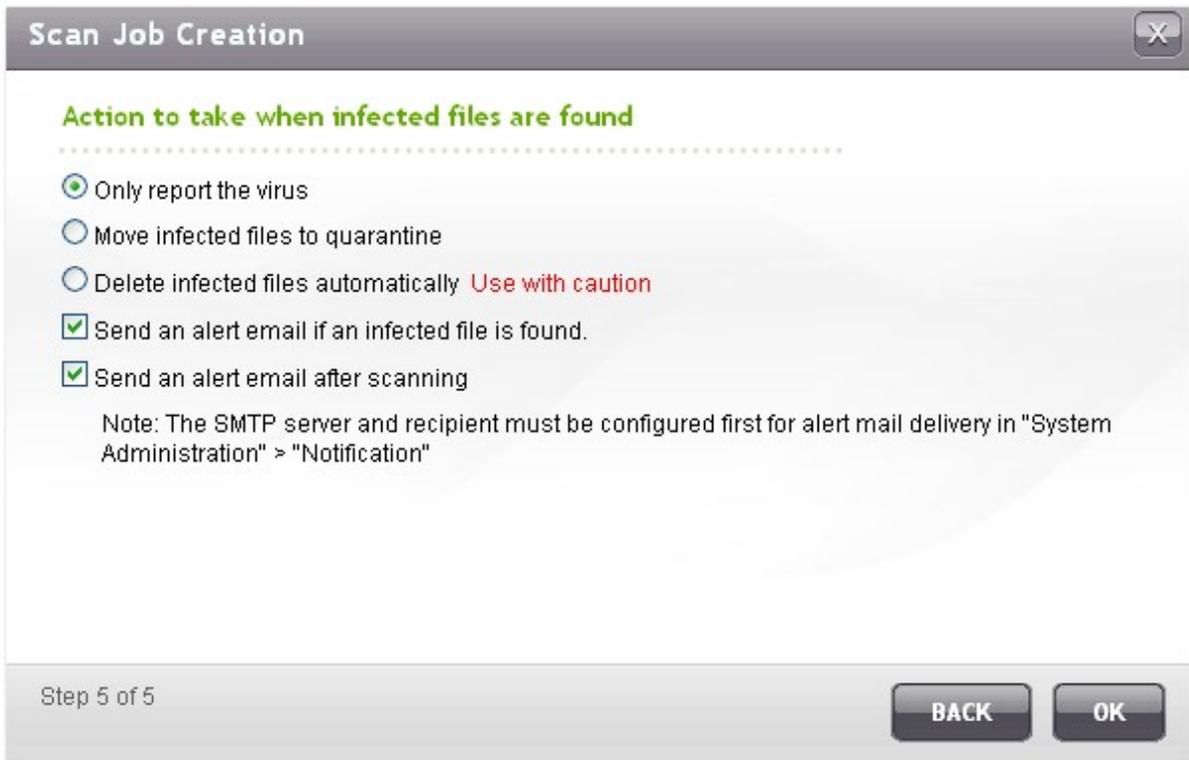
Step 4 of 5

BACK NEXT CANCEL

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.

Antivirus

STATUS SCAN JOBS REPORTS QUARANTINE

Scan Jobs New Scan Job

Job Name	Last Scan	Duration	Infected Files	Action
01	2011/08/22 17:25:38	00:01:45	1	    

Total: 1 | Display 10 entries per page. 1 / 1

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.

Antivirus

STATUS
SCAN JOBS
REPORTS
QUARANTINE

Reports

Job Name	Last Scan	Duration	Infected Files	Action
01	2011/07/26 16:11:50	00:00:21	1	 
01	2011/07/26 16:06:24	00:00:21	1	 
01	2011/07/26 14:15:02	00:00:22	2	 

Total: 3 | Display 10 entries per page. 1 / 1

Number of days to keep the logs: 10

Download all logs DOWNLOAD

Archive logs after expiration. Save the archive files in the folder: /Download

APPLY

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.

Antivirus

STATUS
SCAN JOBS
REPORTS
QUARANTINE

Quarantine

 Restore Selected Files
 Delete Selected Files
 Delete All Files

	File Name	Path	Virus name	Job Name	Action
<input type="checkbox"/>	keyfinder.exe	/Public	Hacktool.Crack.XP	01	  

Total: 1 | Display entries per page.

⏪ ⏩ 1 / 1 ⏪ ⏩

7.16 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".

TFTP Server

TFTP Server

Enable TFTP Server

UDP Port :

You need to specify a root directory for the TFTP server.

Root Directory :

Enable TFTP Logging

The log file(s) will be saved in the selected folder. If the size of a log file exceeds 1MB, the file will be archived automatically.

Save log files in :

Access Right: ▼

Allow TFTP access from :

Anywhere

Certain IP range only

Start IP Address : . . .

End IP Address : . . .

7.17 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 "Applications" > "VPN Service" > "VPN Server Settings". Under "General Settings", select a network interface to connect to the desired network which the NAS belongs to.



The screenshot shows the 'VPN Service' configuration page. At the top, there are three tabs: 'VPN SERVER SETTINGS' (which is active), 'VPN CLIENT MANAGEMENT', and 'CONNECTION LIST'. Below the tabs, the 'General Settings' section is visible. It contains a text instruction: 'Select a network interface to connect to the desired network which the NAS belongs to. You can forward the VPN ports on the router by [Auto Router Configuration](#), and also replace the WAN IP by MyCloudNAS name for connection.' Below this instruction, there is a 'Network Interface:' label followed by a dropdown menu showing 'Ethernet 1+2'. At the bottom of the section, it displays 'MyCloudNAS Name: mcna.mycloudnas.com'.

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.

Note: The default NAS IP is 10.0.0.1 under PPTP VPN connection.

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.

PPTP settings

The PPTP server allows users to access the LAN remotely. Use the default settings or specify the settings manually. To understand more, please check: (http://www.qnap.com/pro_application.asp?ap_id=836)

Enable PPTP VPN server

VPN client IP pool -

[Advanced Settings](#)

OpenVPN Settings

An OpenVPN client software is required on the remote PC. Use the default VPN settings or configure the settings manually. To understand more, please check: (<http://openvpn.net/>)

Enable OpenVPN server

VPN client IP pool -

[Advanced Settings](#)

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 does 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 "Applications" > "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".

The screenshot shows the 'VPN Service' interface with the 'VPN CLIENT MANAGEMENT' tab selected. A table lists two users: 'hikaru' and 'admin'. Both users have a status of 'Ready' and the 'PPTP' checkbox is checked. The 'OpenVPN' checkbox is unchecked for both. A red box highlights the 'Add VPN Users' button in the top right corner of the table area. Below the table, there is a 'Delete' button, a 'Total: 2' indicator, a 'Display 10 entries per page' dropdown, and pagination controls showing '1 / 1'. An 'APPLY' button is located at the bottom right of the interface.

<input type="checkbox"/>	User Name	Status	PPTP	OpenVPN
<input type="checkbox"/>	hikaru	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	admin	Ready	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Select users and their privileges

Create a User

Total: 3

1 / 1

User Name	PPTP	OpenVPN
bbb	<input type="checkbox"/>	<input checked="" type="checkbox"/>
jason	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
rr	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Step 1 / 1

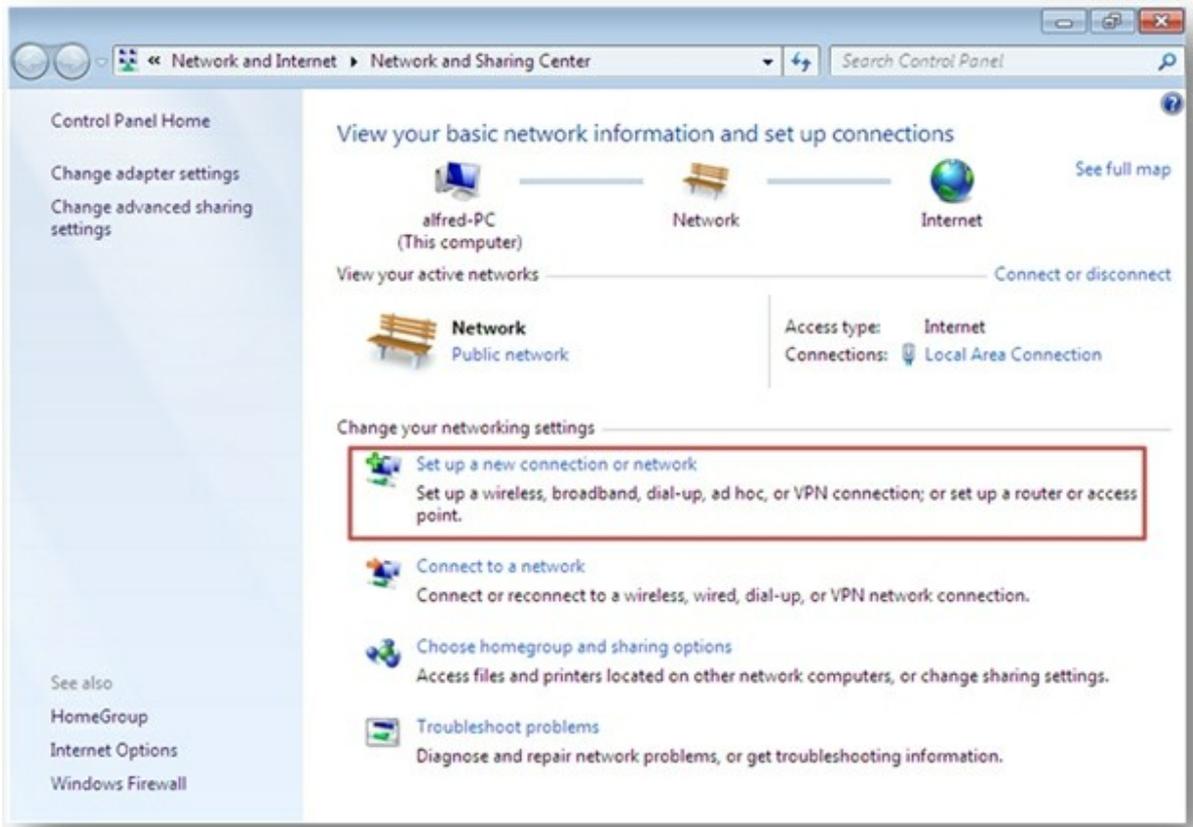
ADD CANCEL

6. Connect to the private network by a VPN client

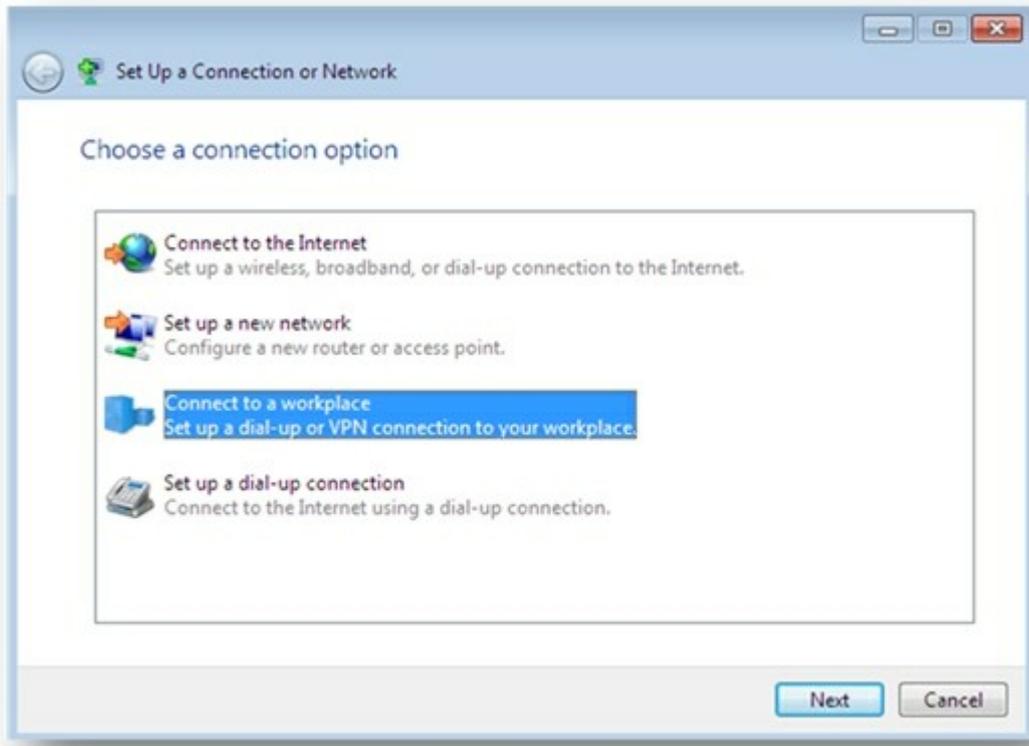
Now you can use your VPN client to connect to the NAS via the VPN service.

PPTP on Windows 7

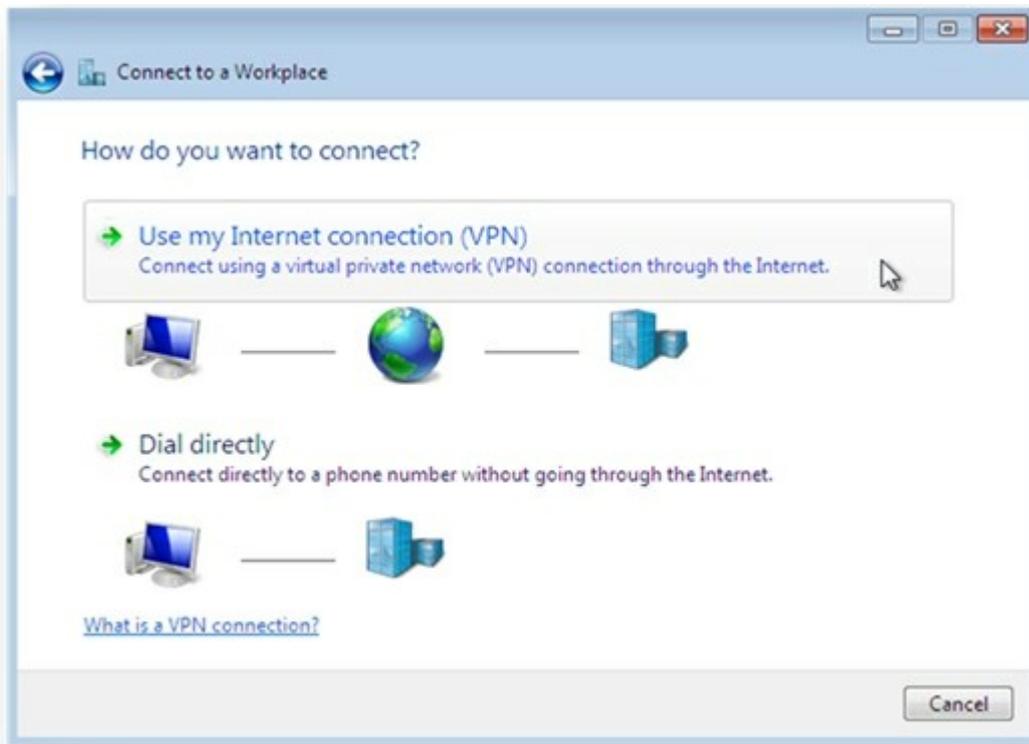
1. Go to "Control Panel" > "Network and Sharing Center". Select "Set up a new connection or network".



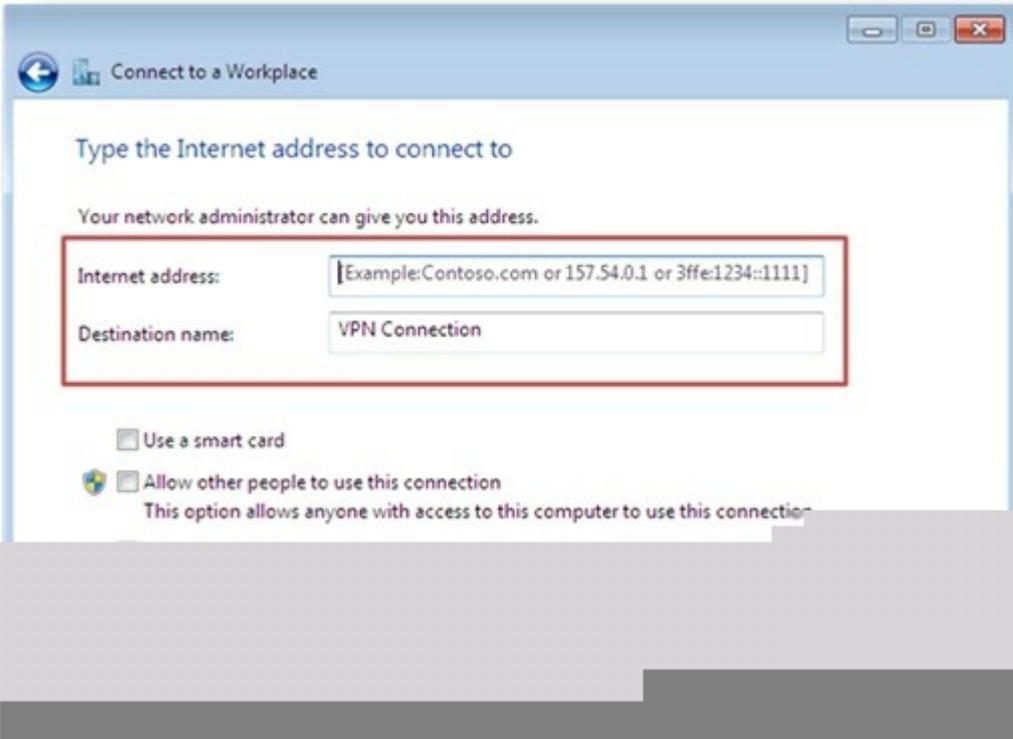
2. Select "Connect to a workplace" and click "Next".



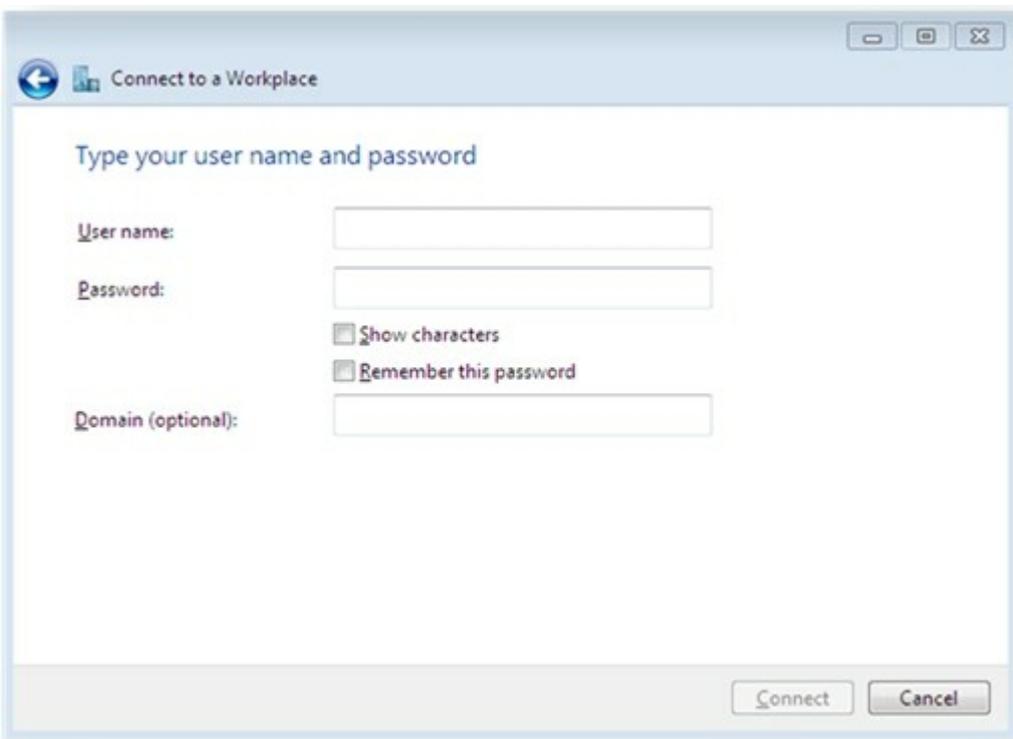
3. Select "Use my Internet connection (VPN)".



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 username and password which is added from the NAS for VPN access. Click "Connect".



PPTP on Mac OS X 10.7

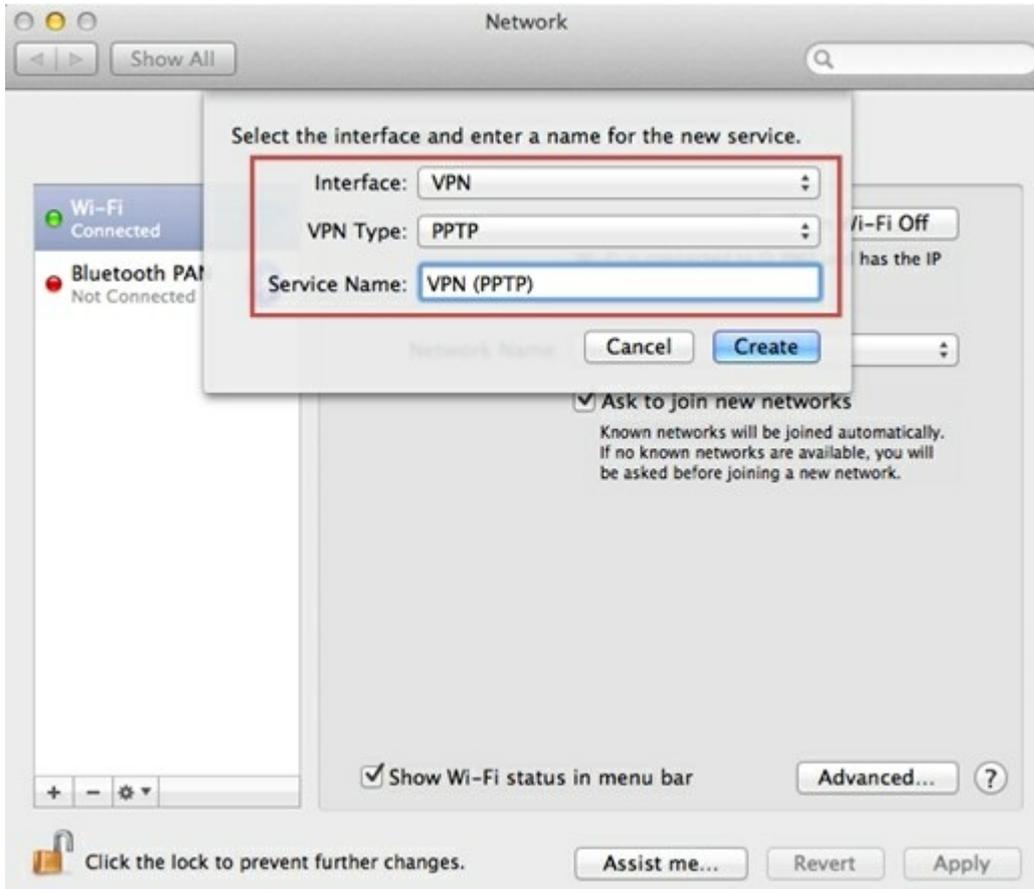
1. Choose "Apple menu" > "System Preferences", and click "Network".



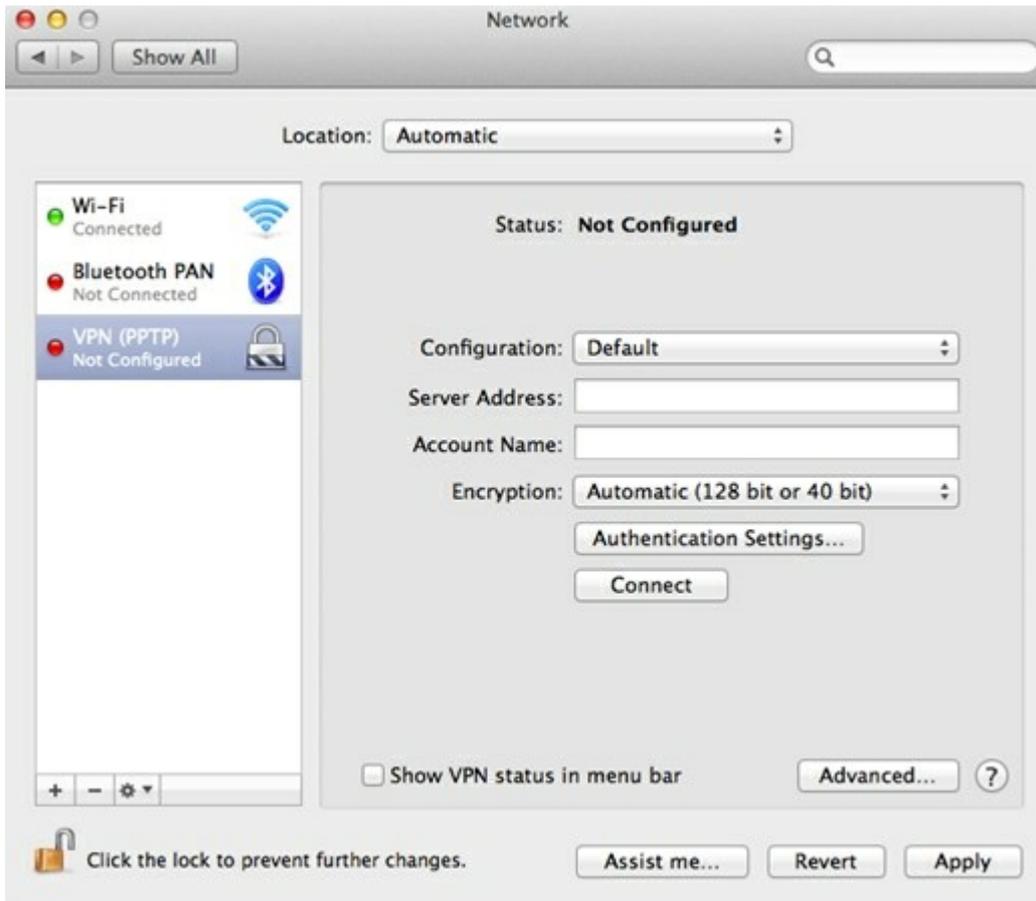
2. Click "Add (+)" at the bottom of the list, and choose "VPN" as the interface.



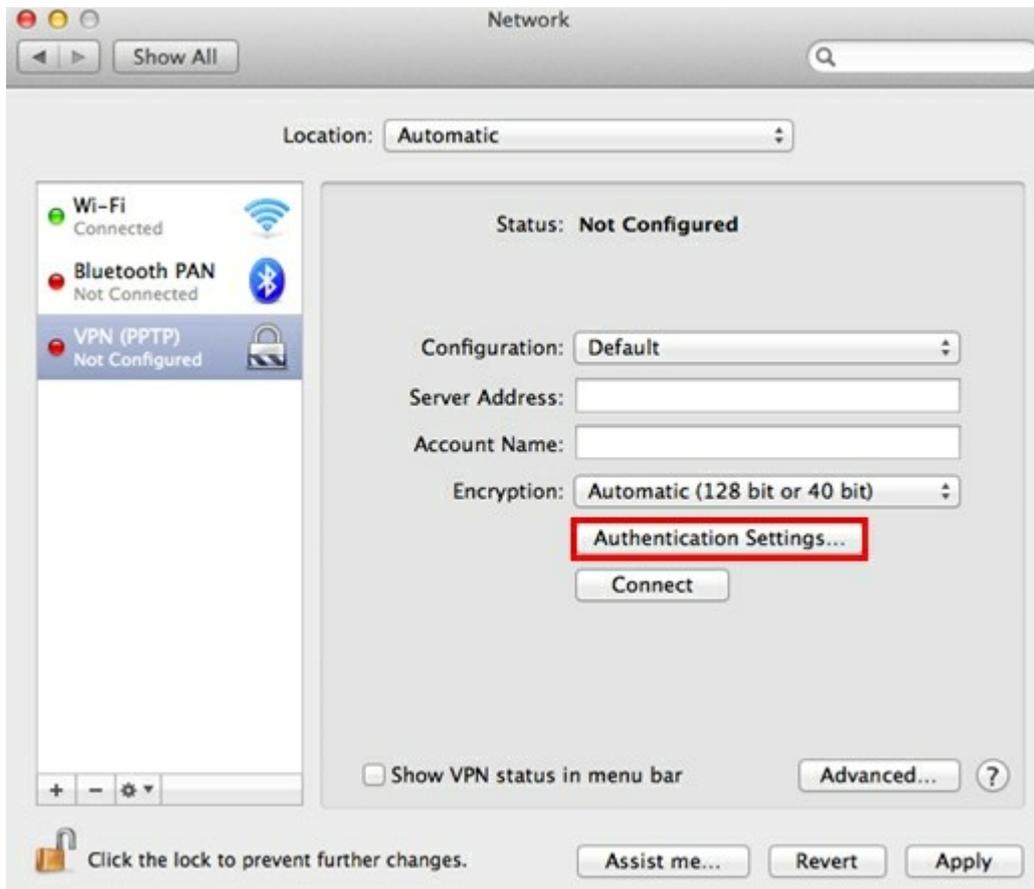
3. Choose the VPN type according to the settings of the NAS to connect. Enter the service name.



4. In "Server Address", enter the MyCloudNAS name or the WAN IP of the NAS. In "Account Name", enter your username which is added from the NAS.



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 ("Applications" > "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 ("Applications" > "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 ("Applications" > "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.

7.18 LDAP Server

The LDAP server of the NAS allows the administrator to create users to access multiple NAS servers with the same username and password. Follow the instructions below to configure the LDAP server.

Enable LDAP Server

Login the NAS as "admin". Go to "Applications" > "LDAP Server" and enable LDAP server. Enter the full LDAP domain name and the password for the LDAP server, then click "Apply".

The screenshot shows the "LDAP Server" configuration page. At the top, there are four tabs: "LDAP SERVER" (selected), "USERS", "GROUPS", and "BACKUP/RESTORE". Below the tabs, the "LDAP Server" section is visible. It includes a checked checkbox for "Enable LDAP Server". The "Full Domain Name" field contains "my-domain.com". The "Password" field is masked with dots. The "Verify Password" field is empty. The "Root DN" is "cn=admin,dc=my-domain,dc=com". The "Users Base DN" is "ou=people,dc=my-domain,dc=com". The "Group Base DN" is "ou=group,dc=my-domain,dc=com". There is an "Initialize" button next to the text "(Delete all users and groups from the LDAP server)". At the bottom right, there is an "APPLY" button.

LDAP Server

LDAP SERVER | **USERS** | **GROUPS** | **BACKUP/RESTORE**

LDAP Server

Enable LDAP Server

Full Domain Name :

Password :

Verify Password :

Root DN : cn=admin,dc=my-domain,dc=com

Users Base DN : ou=people,dc=my-domain,dc=com

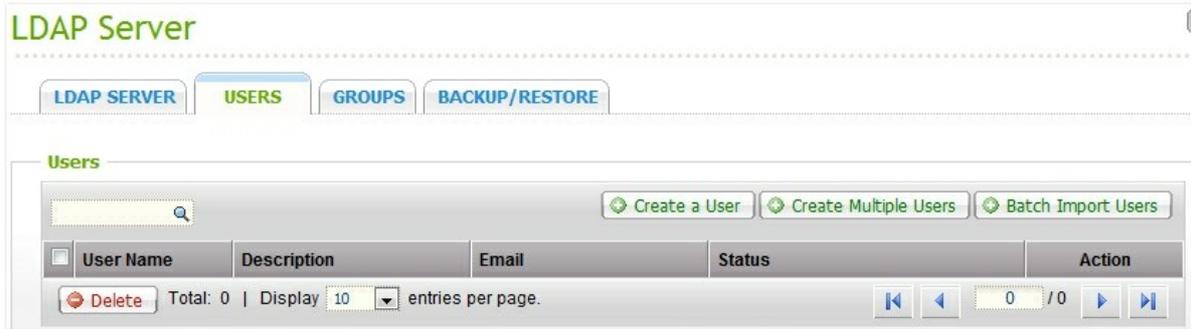
Group Base DN : ou=group,dc=my-domain,dc=com

Initialize LDAP Database : (Delete all users and groups from the LDAP server)

Enable this NAS to be the client of the LDAP service : [Domain Security](#)

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".

Domain Security

Domain Security for File Services

No domain security (local users only)

Active Directory authentication (domain member)

LDAP authentication

Select the type of LDAP server: LDAP server of the local NAS

Apply to set this NAS to be able to use the LDAP server users and group from this QNAP NAS.

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".

Domain Security

Domain Security for File Services

No domain security (local users only)

Active Directory authentication (domain member)

LDAP authentication

Select the type of LDAP server:

Status :

IP address or NAS name:

LDAP domain :

Example: mydomain.local

Password:

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.

LDAP SERVER **USERS** **GROUPS** **BACKUP/RESTORE**

Back up LDAP Database

Back up Database

1. Backup frequency:

2. Start Time: :00

3. Destination folder:

4. Backup options

Overwrite existing backup file (LDAP_Backup.exp)

Create a new file for each backup and append the date to the filename (LDAP_backup_YYYY_MM_DD.exp)

5. Apply

Restore LDAP Database

You can import a backup file to restore the entire LDAP configuration and contents.
Select a backup file to import :

8. Backup

Remote Replication [543](#)

Cloud Backup [569](#)

Time Machine [579](#)

External Drive [584](#)

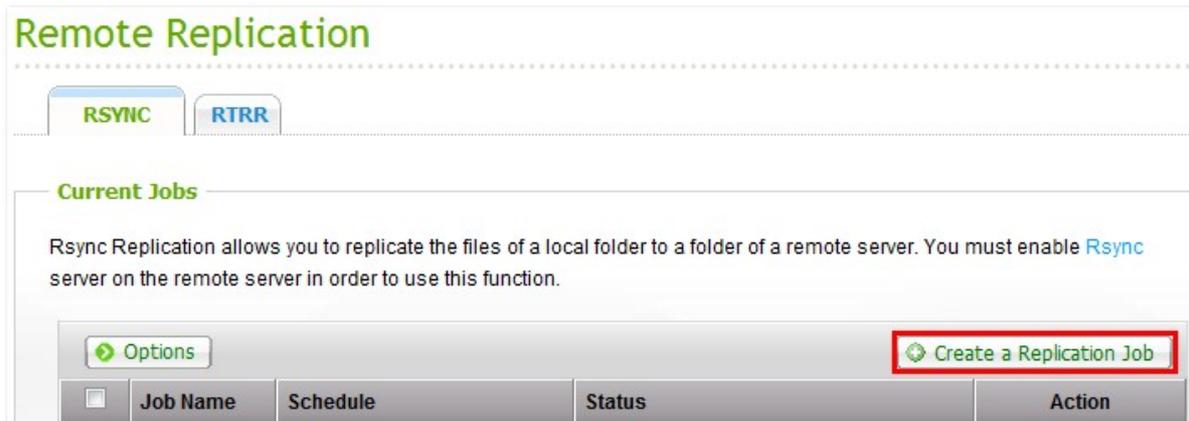
USB One Touch Copy [599](#)

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 "Applications" > "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".



The screenshot displays the 'Remote Replication' web interface. At the top, there are two tabs: 'RSYNC' (selected) and 'RTRR'. Below the tabs, the 'Current Jobs' section contains a descriptive paragraph: 'Rsync Replication allows you to replicate the files of a local folder to a folder of a remote server. You must enable Rsync server on the remote server in order to use this function.' Below this text, there are two buttons: 'Options' and 'Create a Replication Job'. The 'Create a Replication Job' button is highlighted with a red rectangular box. At the bottom of the interface, there is a table with the following columns: Job Name, Schedule, Status, and Action.

	Job Name	Schedule	Status	Action
--	----------	----------	--------	--------

- Specify the server type, NAS or Rsync server, of the remote server. Enter a job name. Click "Next".

Remote Replication

QNAP
TURBO NAS

Remote Replication Wizard

This wizard helps you create a remote replication job. Enter the name of the remote replication job and click **Next**.

Server type: NAS server

Remote Replication Job Name: backup

Step 1 of 7

NEXT CANCEL

- Enter the IP address, port number, username and password to login the remote server. The default port number is 873. Note that the login username 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".

Remote Replication

QNAP
TURBO NAS

Remote Destination

Name or IP address of the remote server: 172.17.20.77

Port Number: 873

User Name: admin

Password: [masked]

Remote Host Testing: TEST

Step 2 of 7

BACK NEXT CANCEL

4. Specify the destination folder, where the data will be replicated to.

Remote Replication

QNAP
TURBO NAS

Remote Destination

Destination Path:
(e.g. /ShareFolder/Directory)

Remain Capacity: 0 Mb

Step 3 of 7

BACK NEXT CANCEL

5. Specify the local folder, where the data will be replicated from.

Remote Replication

QNAP
TURBO NAS

Local Source

Local Path:
(e.g. /ShareFolder/Directory)

Step 4 of 7

BACK NEXT CANCEL

6. Select to replicate the data immediately or specify the backup schedule.

Remote Replication

QNAP
TURBO NAS

Replication Schedule

Select schedule:

Replicate Now

Daily

Weekly

Monthly

Time

Monday

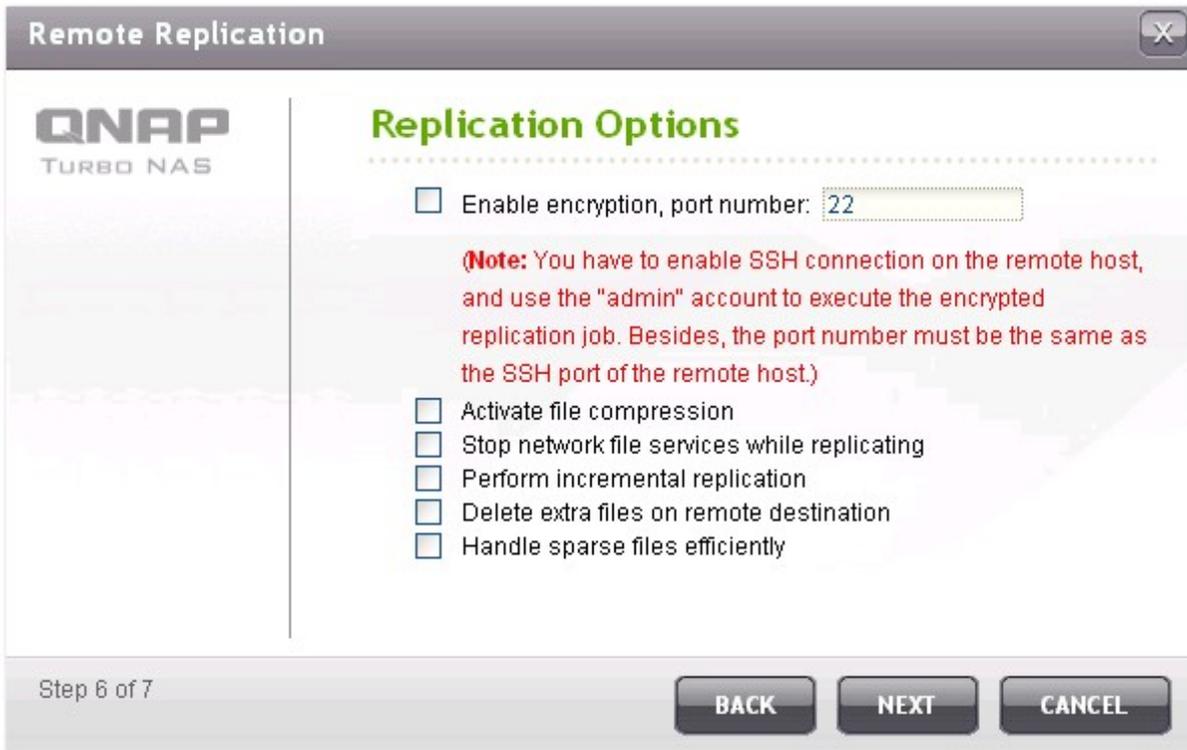
01

00 : 00

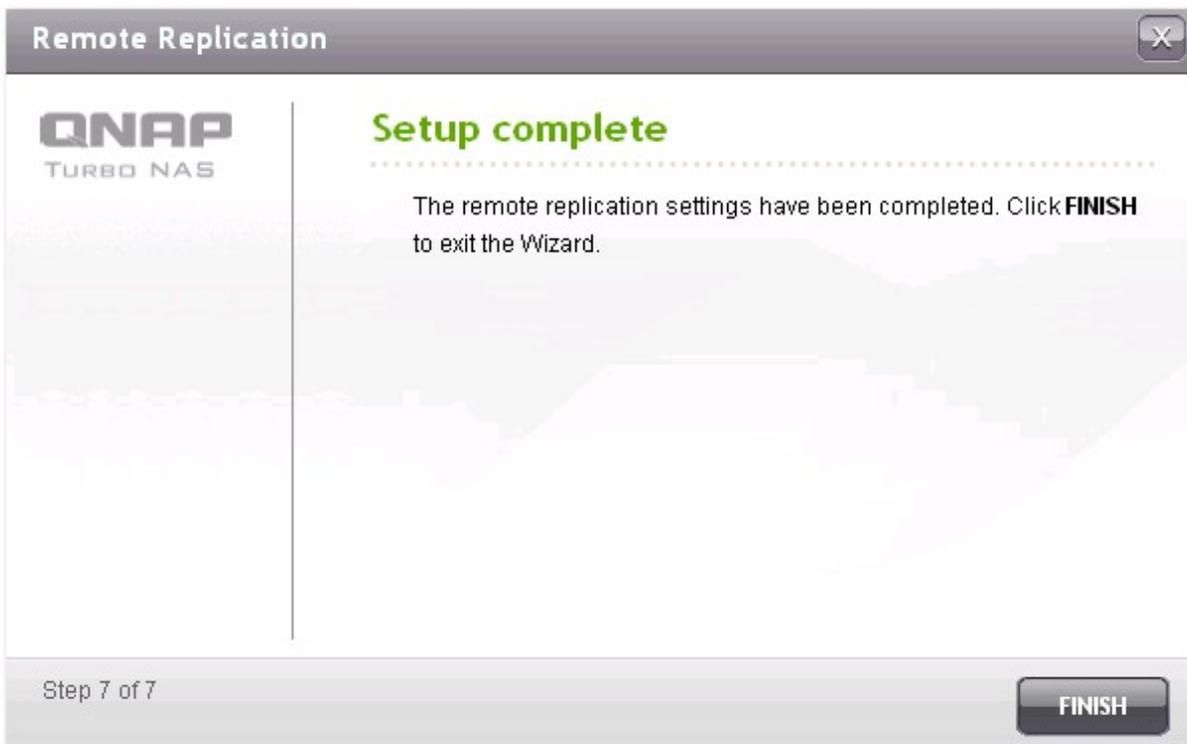
Step 5 of 7

BACK NEXT CANCEL

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.



- 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.



RSYNC RTRR

Current Jobs

Rsync Replication allows you to replicate the files of a local folder to a folder of a remote server. You must enable Rsync server on the remote server in order to use this function.

Options Create New Replication Job

<input type="checkbox"/>	Job Name	Schedule	Status	Action
<input type="checkbox"/>	backup	00:00 - Monthly: 1	Ready	    

Delete

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.



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 ("Applications" > "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*

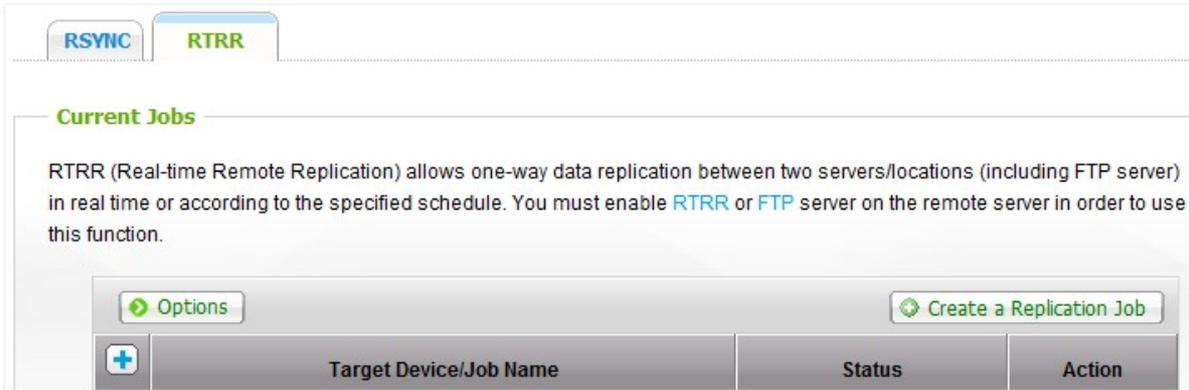
*Each job supports maximum 5 folder pairs.

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".

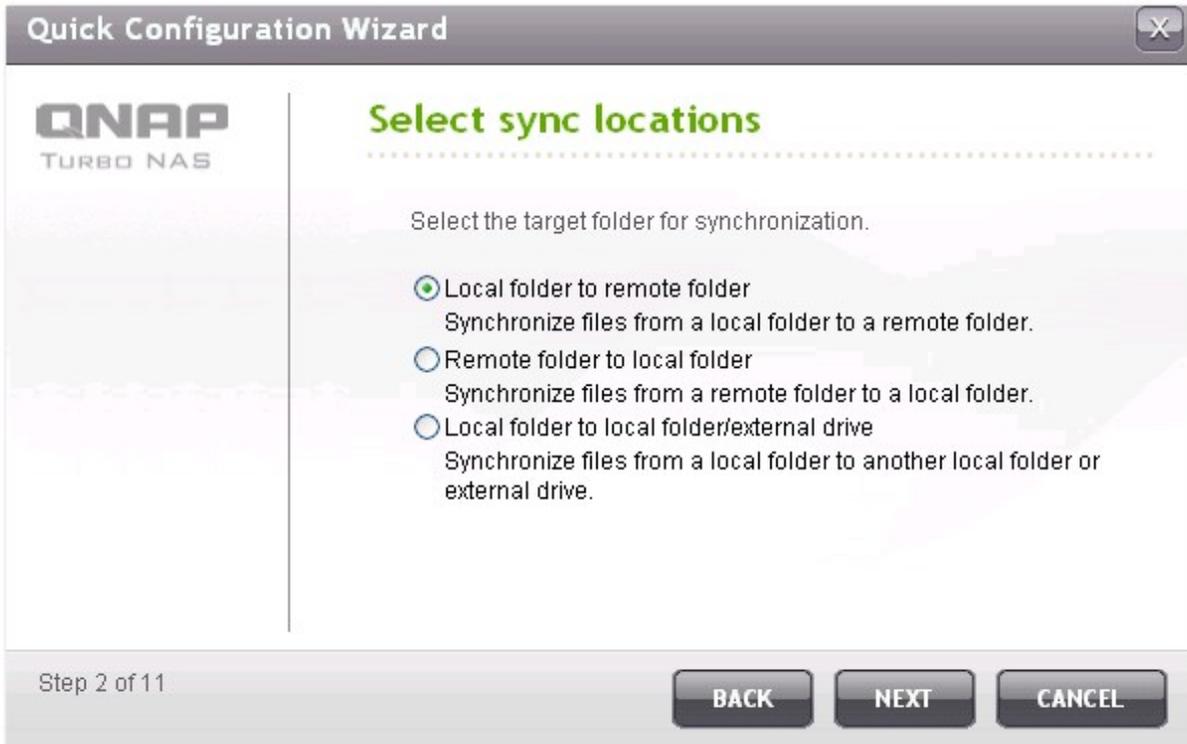


2. When the wizard shows up, click "Next".



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 username and password with read/write access to the server. Click "Next".

Quick Configuration Wizard

QNAP
TURBO NAS

Configure Remote Host Settings

IP Address/Host Name: ✓

Server Type: ?

Port:

FTP with SSL/TLS (Explicit)

Passive Mode

User Name: ✓

Password: ✓

Step 3 of 11

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".

Quick Configuration Wizard

QNAP
TURBO NAS

Configure Remote Host Settings

IP Address/Host Name: ✓

Server Type: ?

Port: Enable Secure Connection (SSL)

Password: ✓

TEST

Step 3 of 11

BACK **NEXT** **CANCEL**

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.

Quick Configuration Wizard

QNAP
TURBO NAS

Replication Options

Real-time
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.

Schedule
Scheduled synchronization copies files that are new, changed, and renamed from the source folder to the target folder according to the pre-configured schedule.

Replicate Now ▾

Configure policy and filter

Step 6 of 11

BACK NEXT CANCEL

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.

Quick Configuration Wizard

Configure synchronization filter

File size ? File date/time ?

Min size: 0 KB From: 2000 / 01 / 01

Max size: 1000 MB To: 2012 / 01 / 01

Include file types ?

Documents Pictures Video Applications Music

Temporary files Others:

Exclude file types ?

Documents Pictures Video Applications Music

Temporary files Others:

Step 8 of 11

BACK **NEXT** **CANCEL**

10. Enter a job name. Click "Next".

The screenshot shows a window titled "Quick Configuration Wizard" with a close button (X) in the top right corner. On the left side, there is the QNAP TURBO NAS logo. The main area is titled "Enter a sync job name" in green. Below the title, there is a text input field for "Job Name" containing the text "Recordings-->Remote:Qdownload" and a green checkmark icon to its right. Below the input field, there is a note: "Specify a name for the sync job. It is a required field and cannot be empty." At the bottom of the window, it says "Step 9 of 11" and has three buttons: "BACK", "NEXT", and "CANCEL".

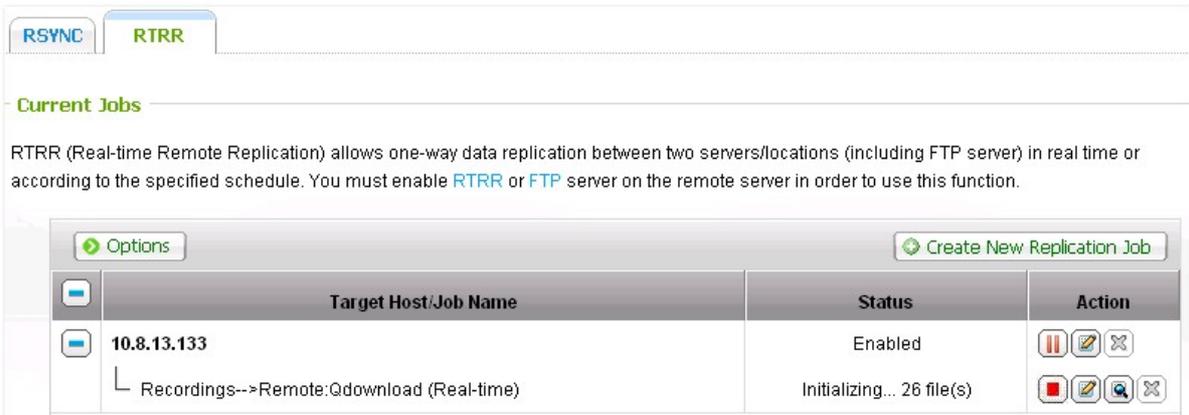
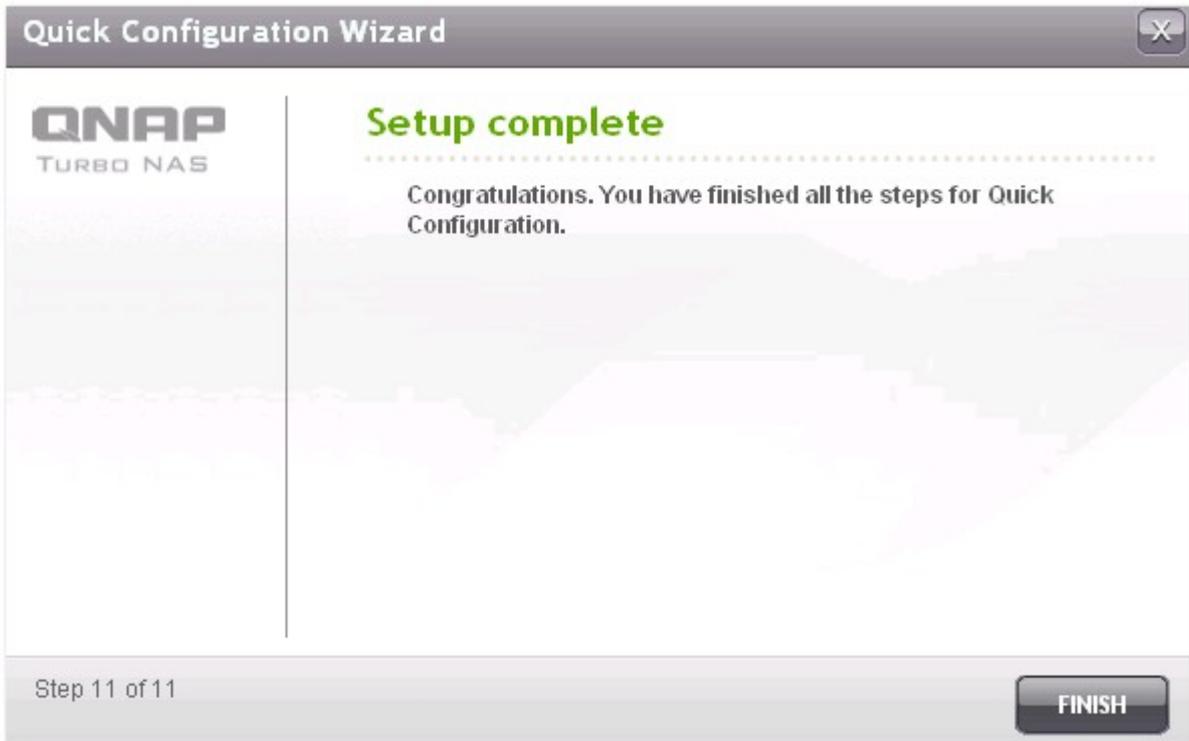
11. Confirm the settings and click "Next".

The screenshot shows a window titled "Quick Configuration Wizard" with a close button (X) in the top right corner. On the left side, there is the QNAP TURBO NAS logo. The main area is titled "Confirm Settings" in green. Below the title, there is a list of settings with a vertical scrollbar on the right. The settings are:

Job Name:	Recordings-->Remote:Qdownload
Folder Pair Number:	2
Folder Pairs 1:	[/Recordings] --> [/Qdownload]
Folder Pairs 2:	[/Download] --> [/Qdownload]
Server Type:	Local folder to remote folder
Server Type:	FTP Server
Host Name:	10.8.13.133:21
User Name	test
Schedule Type	Real-time
Policy:	Timeout (second): 120 Number of retries: 3 Retry Intervals (second): 60
File size:	--- ~ 1000 mb Pictures

At the bottom of the window, it says "Step 10 of 11" and has three buttons: "BACK", "NEXT", and "CANCEL".

12. Click "Finish" to exit the wizard.



Icon	Description
	<ul style="list-style-type: none"> • Enable connection to a remote server. • Start a replication job.
	<p>Stop connection to a remote server or external drive.</p>
	<p>Stop a replication job.</p>
	<p>View job status and logs; download logs.</p>
	<ul style="list-style-type: none"> • Edit the connection settings of a remote server. • Edit the settings of a replication job.
	<ul style="list-style-type: none"> • Delete connection settings to a remote server. • Delete a replication job. <p>This button is available only after a replication job is stopped or the connection to the remote server is stopped.</p>

To edit the replication job properties, click "Options".

	Target Host/Job Name	Status	Action
+	10.8.13.133	Enabled	

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").

Customize job property

EVENT LOGS | POLICY | FILTER

Download Detailed Logs
Maximum Log Size (MB): MB (Max 1GB)
Enable this option to include more information in the log file. You can also specify the maximum file size.

Send an alert email in the following condition(s):
 Synchronization failed
 Synchronization has completed.
Enable this option to allow the system to send an alert email to the system administrator when a synchronization job fails or completes.

Note: The SMTP server must be configured first for alert mail delivery. [Click this to configure the SMTP server](#)

APPLY CANCEL

Specify the replication policy in "Policy" and filter settings in "Filter". These will become the default settings for all RTRR replication jobs.

Customize job property [X]

EVENT LOGS | **POLICY** | **FILTER**

- Delete extra files ?
- Detect sparse files ?
- Check file contents ?
- Compress files during transmission ?
- Ignore symbolic links ?
- Extended attributes ?

Timeout and retry settings: ?

Timeout (second): 120

Number of retries: 3

Retry Intervals (second): 60

APPLY **CANCEL**

Download replication job logs:

To view the status and logs of a replication job, click .

Options		Create New Replication Job	
	Target Host/Job Name	Status	Action
	10.8.13.133	Disable	
	└ Recordings-->Remote:Qrecordings (Schedule: Weekly Monday 00:00)	Failed (Check the log for detail)	

You can view the details of a replication job.

Job Status and Logs

JOB STATUS | **JOB LOGS**

Job Name: Recordings-->Remote:Qrecordings

Schedule Type: Schedule: Weekly Monday 00:00 **Folder Pairs:** 1

Total File(s): ----- **Total Folder(s):** -----

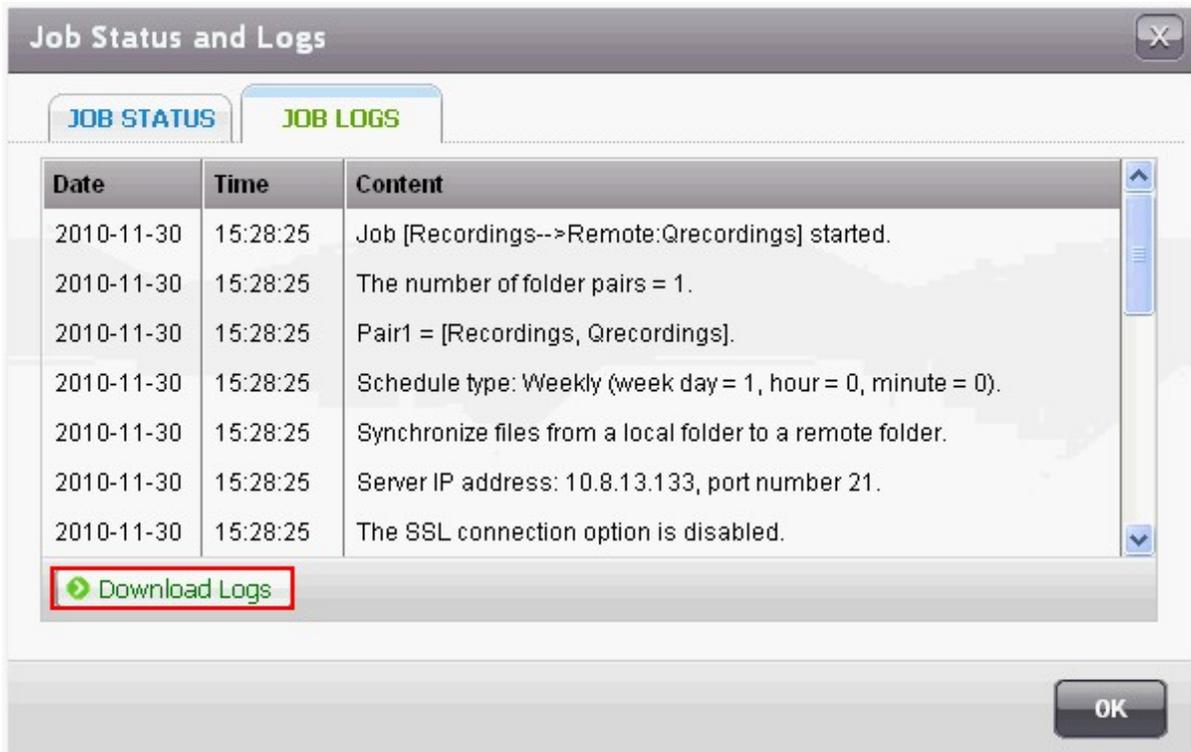
Total File Size: ----- **Average Transmit Speed:** 0 KB

Elapsed Time: 00:00:00 **Time Left:** 00:00:00

Status: Failed

OK

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.



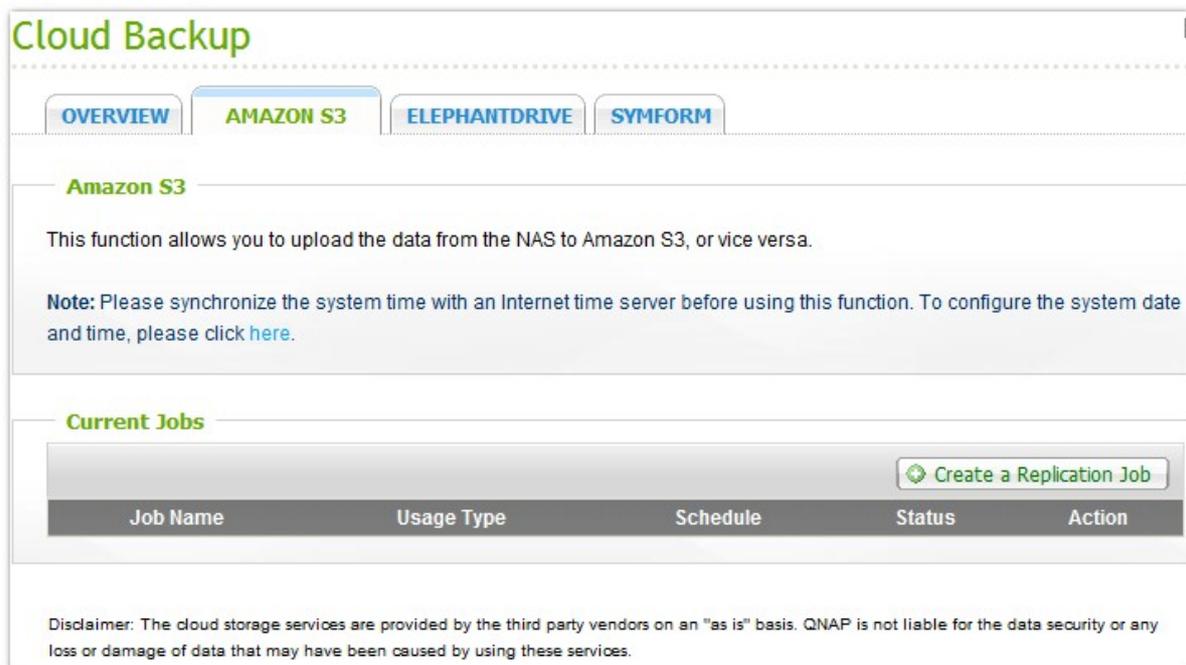
8.2 Cloud Backup

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.

Note: The maximum file size limit is 2GB.



The screenshot shows a web interface titled "Cloud Backup". At the top, there are four tabs: "OVERVIEW", "AMAZON S3" (which is selected and highlighted in green), "ELEPHANTDRIVE", and "SYMFORM". Below the tabs, the "Amazon S3" section is active. It contains the following text:

Amazon S3

This function allows you to upload the data from the NAS to Amazon S3, or vice versa.

Note: Please synchronize the system time with an Internet time server before using this function. To configure the system date and time, please click [here](#).

Current Jobs

On the right side of the "Current Jobs" section, there is a button labeled "Create a Replication Job" with a green plus icon.

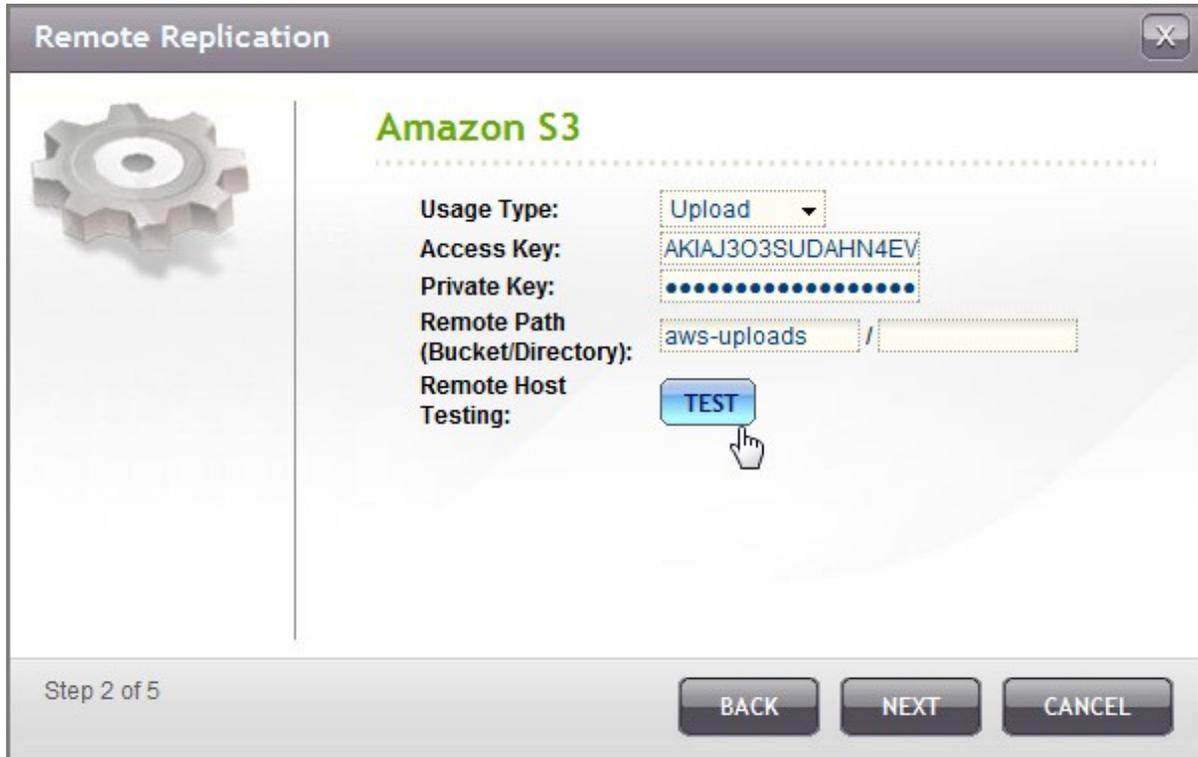
Job Name	Usage Type	Schedule	Status	Action
----------	------------	----------	--------	--------

At the bottom of the interface, there is a disclaimer:

Disclaimer: The cloud storage services are provided by the third party vendors on an "as is" basis. QNAP is not liable for the data security or any loss or damage of data that may have been caused by using these services.

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".

OVERVIEW **AMAZON S3** **ELEPHANTDRIVE** **SYMFORM**

ElephantDrive Account

Enable ElephantDrive Service

ElephantDrive Service

E-mail:

Password:

Verify Password:

Key Features:

- Military grade encryption
- Automatic backups
- Easy to use file sharing
- Access files from anywhere

If you do not have an ElephantDrive account, enter the above information and click "CREATE" to create an account.

Sign up ElephantDrive services from QNAP for a free 30-day trial plus 10% off for 3 months.

Status: -----



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.

ElephantDrive Account

Enable ElephantDrive Service

ElephantDrive Service 

E-mail:

Password:

Verify Password:

If you do not have an ElephantDrive account, enter the above information and click "CREATE" to create an account. CREATE

Sign up ElephantDrive services from QNAP for a free 30-day trial plus 10% off for 3 months.

Status: **Logged in**

For account management and data backup, please go to ElephantDrive website. <https://www.elephantdrive.com/qnap>

APPLY

Login your ElephantDrive account. You can manage the backup and restore jobs on the website (<https://www.elephantdrive.com/qnap>).

Already a User [Login here](#)
English (US) ▾

PROTECT YOUR TURBO NAS FILES WITH ONLINE BACKUP



ElephantDrive: Optimized for Turbo NAS

-  **Continuous Data Protection**
ElephantDrive watches for changes in real-time and provides immediate protection for new or modified files.
-  **Web-based Management**
Check transfer history, modify configurations, change scheduling and select backup sources from any browser-based location in real-time.
-  **Device-integrated Cloud Backup**
You can run ElephantDrive directly on your storage device.
-  **Quick and easy data recovery and restore**
Sign on and browse to the files you need and restore them to your Turbo NAS with a click.

Plans start from **\$9.95** [FREE TRIAL](#) →

30-Day FREE trial just for QNAP users!

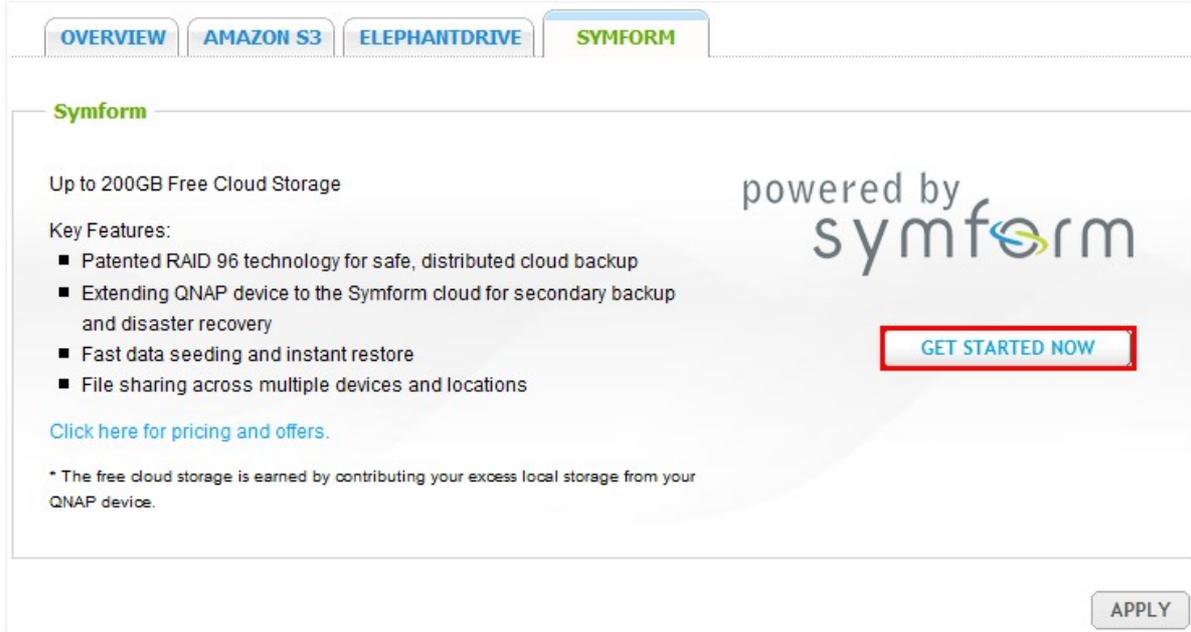
“...a simple, enterprise-class solution for Internet- or cloud-based data protection...” 

To learn more about ElephantDrive, [click here](#). To compare the different ElephantDrive account types, [click here](#)

Copyright © 2011 [ElephantDrive](#). All rights reserved.

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.



The screenshot shows a web interface with four tabs: OVERVIEW, AMAZON S3, ELEPHANTDRIVE, and SYMFORM. The SYMFORM tab is active. The main content area features the Symform logo and the text "powered by symform". Below this, there is a "GET STARTED NOW" button highlighted with a red border. To the left of the button, there is a list of key features and a link for pricing and offers. At the bottom right of the main content area, there is an "APPLY" button.

Symform

Up to 200GB Free Cloud Storage

Key Features:

- Patented RAID 96 technology for safe, distributed cloud backup
- Extending QNAP device to the Symform cloud for secondary backup and disaster recovery
- Fast data seeding and instant restore
- File sharing across multiple devices and locations

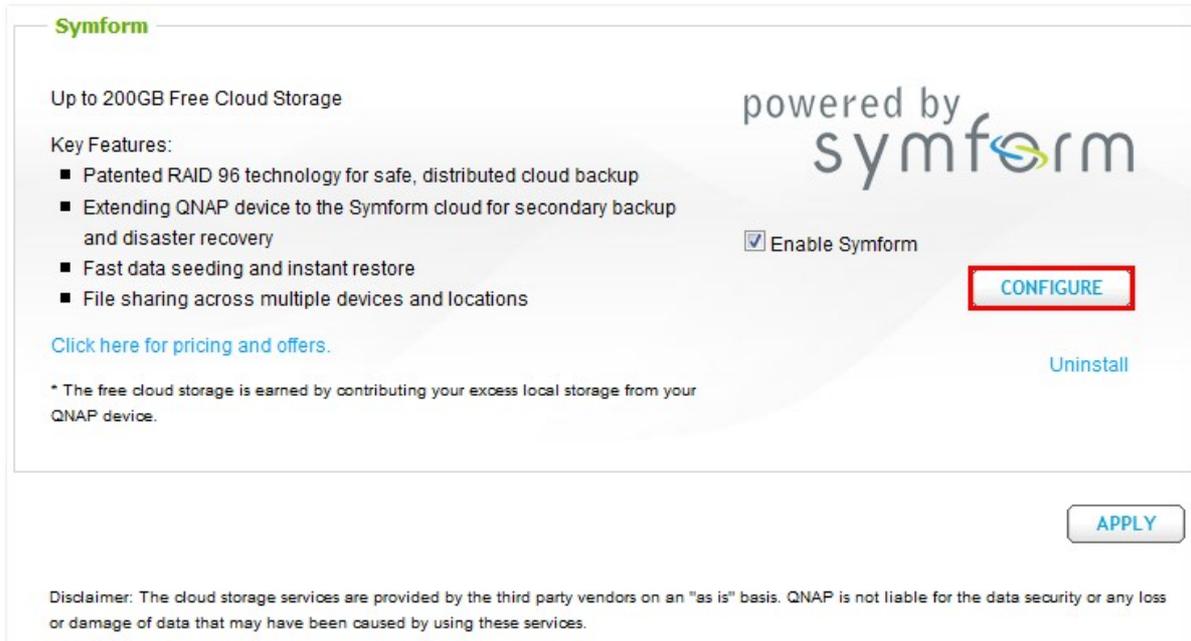
[Click here for pricing and offers.](#)

* The free cloud storage is earned by contributing your excess local storage from your QNAP device.

GET STARTED NOW

APPLY

Click "Configure".



The screenshot shows the same web interface as the previous one, but with the "CONFIGURE" button highlighted with a red border. Additionally, there is a checkbox labeled "Enable Symform" which is checked. Below the "CONFIGURE" button, there is a link for "Uninstall". At the bottom right of the main content area, there is an "APPLY" button. At the bottom of the page, there is a disclaimer.

Symform

Up to 200GB Free Cloud Storage

Key Features:

- Patented RAID 96 technology for safe, distributed cloud backup
- Extending QNAP device to the Symform cloud for secondary backup and disaster recovery
- Fast data seeding and instant restore
- File sharing across multiple devices and locations

[Click here for pricing and offers.](#)

* The free cloud storage is earned by contributing your excess local storage from your QNAP device.

Enable Symform

CONFIGURE

Uninstall

APPLY

Disclaimer: The cloud storage services are provided by the third party vendors on an "as is" basis. QNAP is not liable for the data security or any loss or damage of data that may have been caused by using these services.

Enter your email address and click "Sign-In" to activate Symform on the NAS. An activation code will be sent to this address.

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:

Sign-In

Check your email to get the activation code and finish the setup.

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](#).

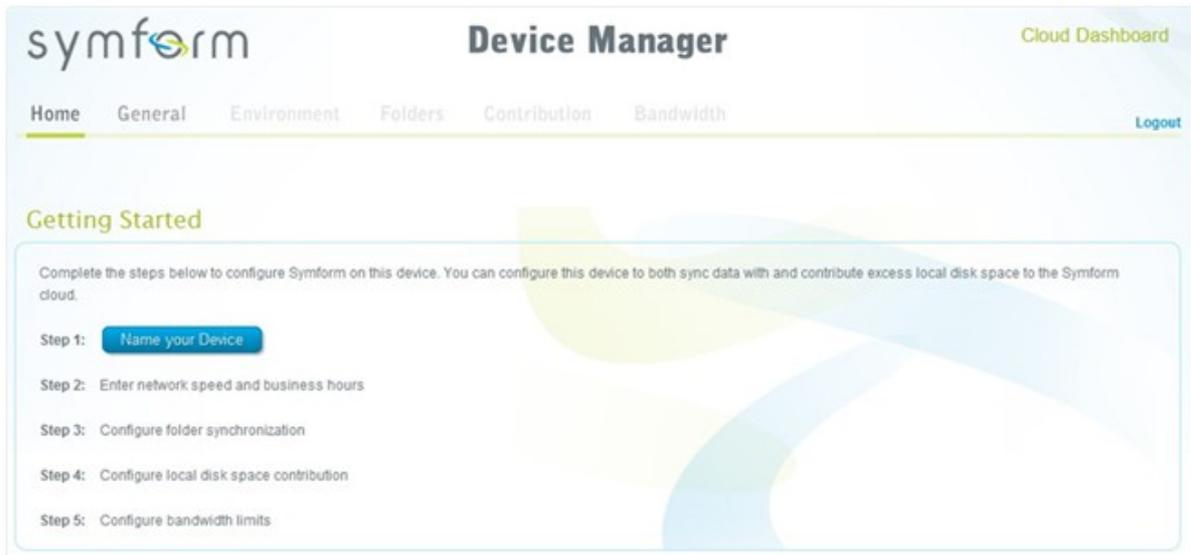
Please enter your Email:

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:	<input type="text"/>	*
First Name:	<input type="text"/>	*
Last Name:	<input type="text"/>	
Password:	<input type="password"/>	*
Confirm Password:	<input type="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.

Time Machine

TIME MACHINE SUPPORT **MANAGE BACKUP**

Time Machine support

After enabling the Time Machine function , you can use the NAS as one of the Mac OS X Time Machine backup destinations.

Enable Time Machine support

Display Name: TMBBackup

User Name: TimeMachine

Password:

Volume: RAID 5 Disk Volume: Drive 1 2 3 Free Size:272GB

Capacity: GB (0 means unlimited)

Note: When using the Time Machine function, AFP service will be enabled automatically. Note that all the Time Machine users share the same network share for this function.

To use this function, follow the steps below.

Configure the settings on the NAS:

1. Enable Time Machine support.

Time Machine support

After enabling the Time Machine function , you can use the NAS as one of the Mac OS X Time Machine backup destinations.

Enable Time Machine support

Display Name: TMBBackup

User Name: TimeMachine

Password:

Volume: RAID 5 Disk Volume: Drive 1 2 3 Free Size:272GB

Capacity: GB (0 means unlimited)

Note: When using the Time Machine function, AFP service will be enabled automatically. Note that all the Time Machine users share the same network share for this function.

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.

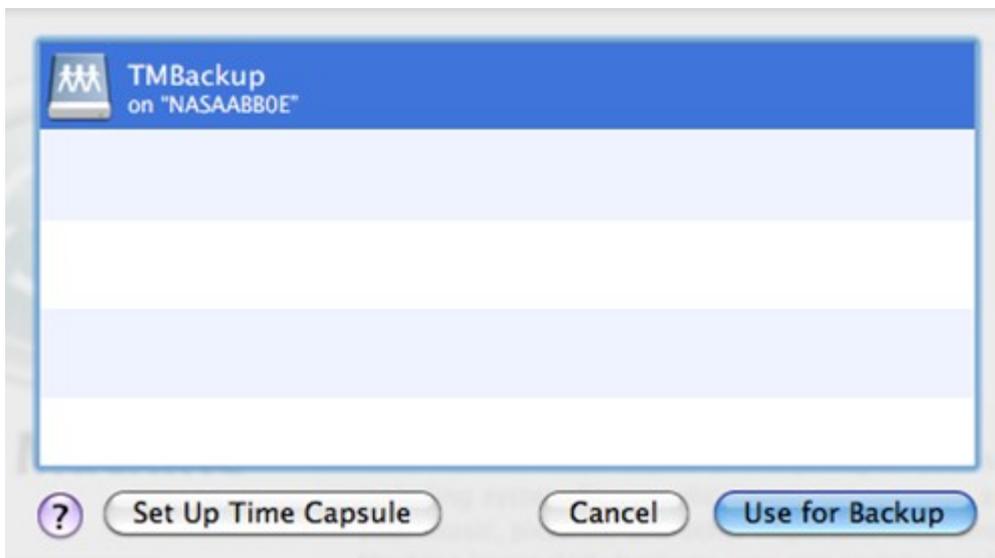
All the Time Machine users share the same network share for this function.

Configure the backup settings on Mac:

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



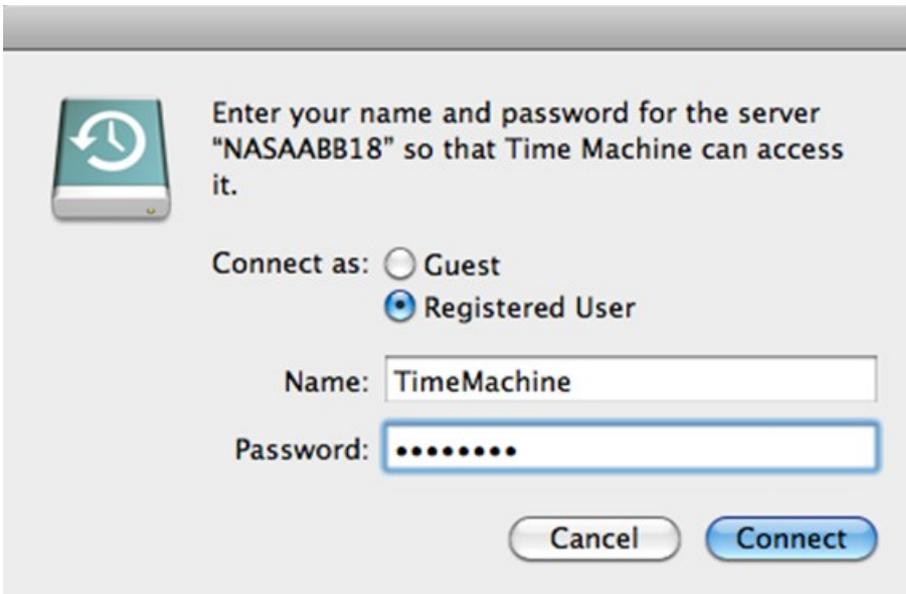
2. Select the TMBBackup on your NAS from the list and click "Use for Backup".



3. Enter the username and password to login the QNAP NAS. Then click "Connect".

Registered username: TimeMachine

Password: The password you have configured on the NAS. It is empty by default.



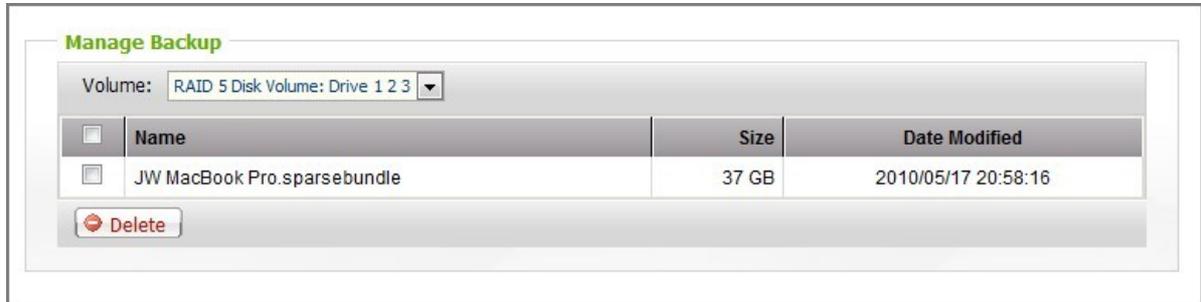
4. Upon successful connection, the Time Machine is switched "ON". The available space for backup is shown and the backup will start in 120 seconds.



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.



The screenshot shows a web interface titled "Manage Backup". At the top, there is a "Volume:" label followed by a dropdown menu showing "RAID 5 Disk Volume: Drive 1 2 3". Below this is a table with three columns: "Name", "Size", and "Date Modified". The table contains one row with the following data: "JW MacBook Pro.sparsebundle", "37 GB", and "2010/05/17 20:58:16". Below the table is a "Delete" button with a red trash icon.

<input type="checkbox"/>	Name	Size	Date Modified
<input type="checkbox"/>	JW MacBook Pro.sparsebundle	37 GB	2010/05/17 20:58:16

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".

External Drive

Current Jobs

The backup function allows you to replicate the data between the local disk volume and an external storage device. You can create a backup job and map it to a specific disk volume. The external storage device with backup job assigned can always be recognized by the NAS whichever the USB or eSATA interface it is connected to.

[Options](#) [Create a new job](#)

	Target Device/Job Name	Status	Action
--	------------------------	--------	--------

3. When the wizard is shown, read the instructions carefully and click "Next".



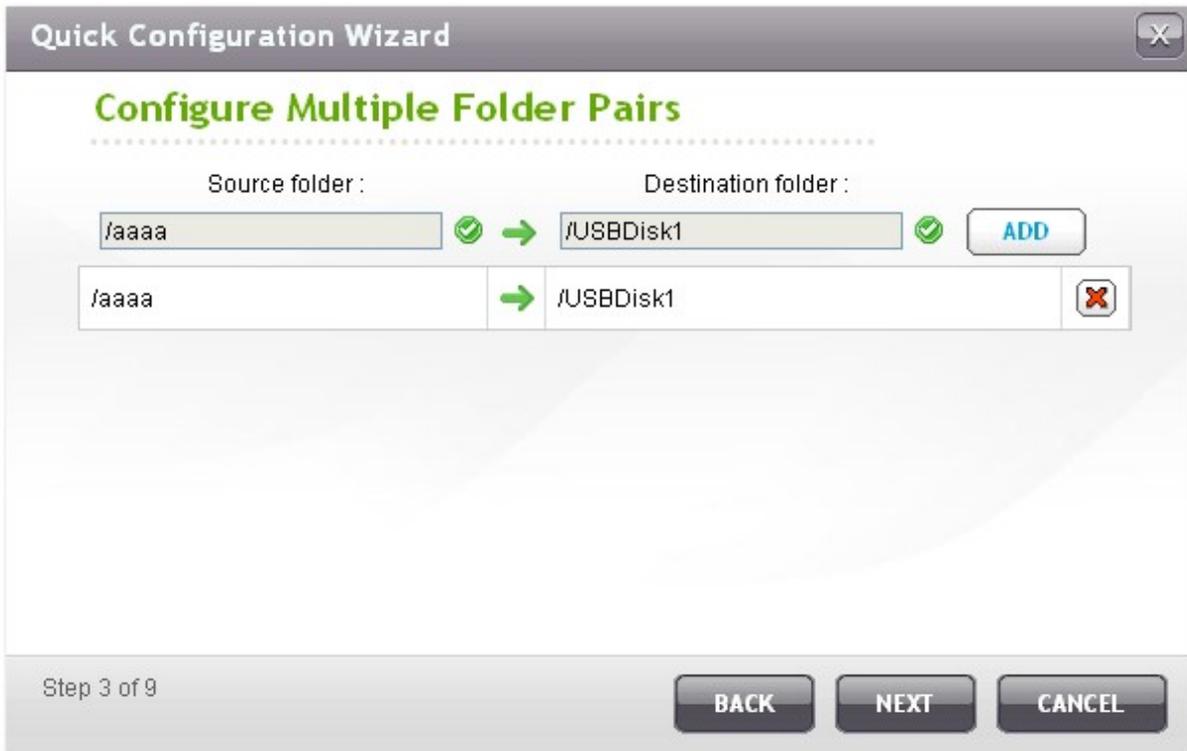
4. Select the backup locations.
 - a. Select an external disk volume* from the drop-down menu. The NAS supports EXT3, EXT4, FAT, NTFS, and HFS+ file systems. The general information of the storage device will be shown.
 - b. Select "Map this backup job to the volume ID only" to map the backup job to 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.

The screenshot shows a window titled "Quick Configuration Wizard" with a close button in the top right corner. On the left side, there is the QNAP logo and the text "TURBO NAS". The main area is titled "Select sync locations" in green. Below the title, it says "Select the target folder for synchronization." and "Select a disk volume:" followed by a dropdown menu showing "USBDisk1". Below the dropdown, the following information is displayed: "Manufacturer: USB 2.0", "Model: Flash Disk", "File System: EXT4", "Size: 1.84 GB / 1.91 GB", and "Volume ID: 26101c59-1c04-473b-baff-036caaab27b5". There are two checkboxes: the first is checked and labeled "Map this backup job to the volume ID only", and the second is unchecked. Below these are two radio buttons: the first is selected and labeled "From local disk to external storage", and the second is unselected and labeled "From external storage to local disk". At the bottom left, it says "Step 2 of 9". At the bottom right, there are three buttons: "BACK", "NEXT", and "CANCEL".

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.

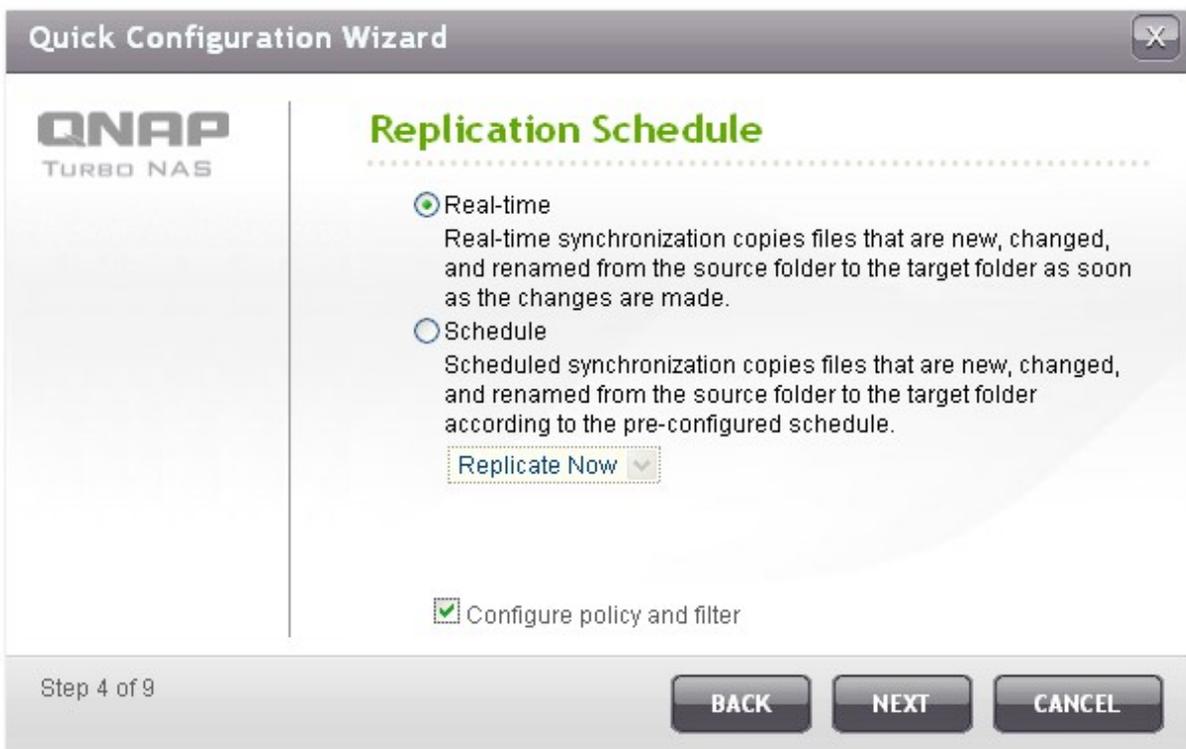


6. Choose between real-time and scheduled backup. Real-time backup copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup.

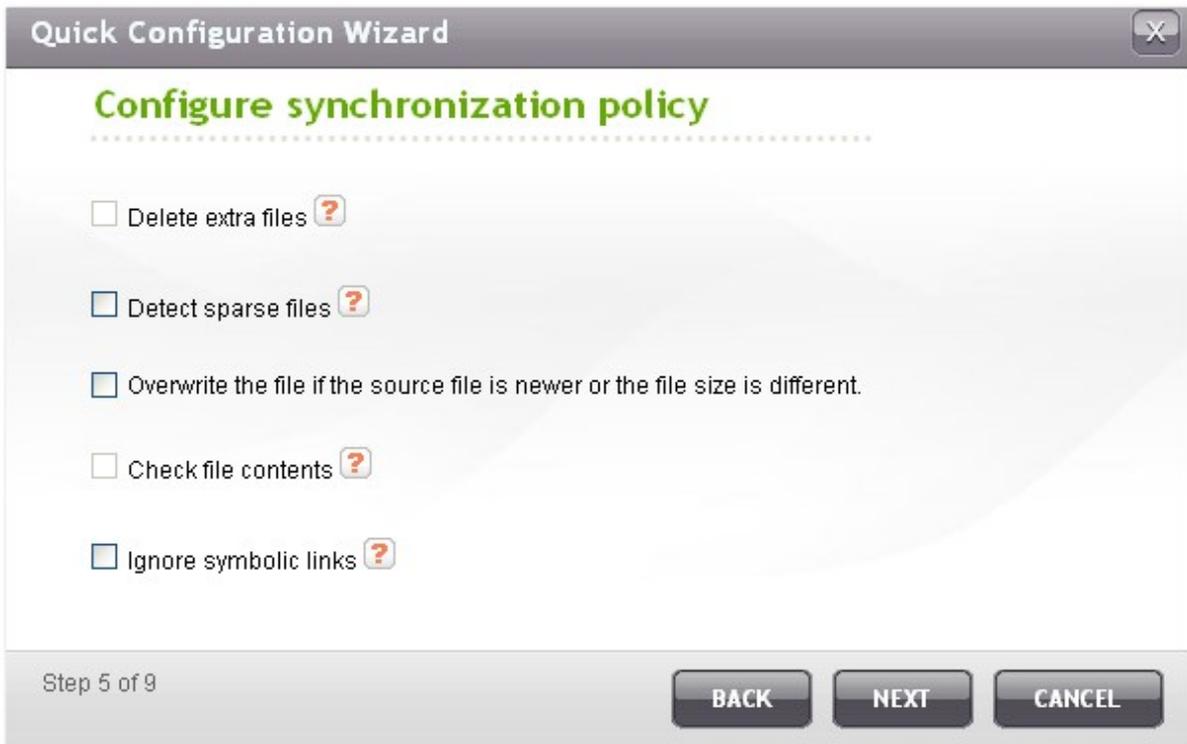
Scheduled backup copies files from the source folder to the target folder according to the schedule. The options are:

- 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.

Quick Configuration Wizard

Configure synchronization filter

File size ? File date/time ?

Min size: 0 KB From: 2000 / 01 / 01

Max size: 1000 KB To: 2012 / 01 / 01

Include file types ?

Documents Pictures Video Applications Music

Temporary files Others:

Exclude file types ?

Documents Pictures Video Applications Music

Temporary files Others:

Step 6 of 9

BACK **NEXT** **CANCEL**

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".

Quick Configuration Wizard

QNAP
TURBO NAS

Enter a sync job name

Job Name: ✓

Specify a name for the sync job. It is a required field and cannot be empty.

Step 7 of 9

BACK NEXT CANCEL

10. Confirm the settings and click "Next".

Quick Configuration Wizard

QNAP
TURBO NAS

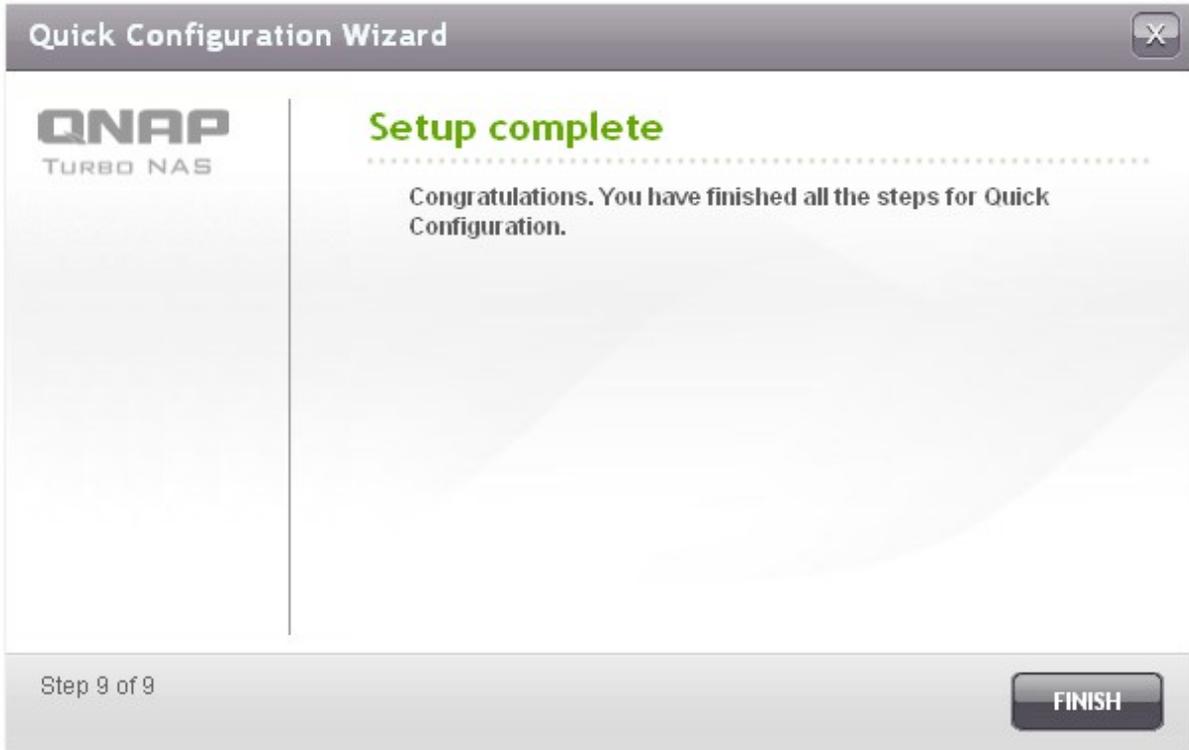
Confirm Settings

Job Name:	aaaa-->USBDisk1
Folder Pair Number:	1
Folder Pairs 1:	[/aaaa] --> [/USBDisk1]
Schedule Type	Real-time
Policy:	
File size:	--- ~ 1000 kb
Exclude file types:	Temporary files

Step 8 of 9

BACK NEXT CANCEL

11. Click "Finish" to exit the wizard.



12. The backup job and the status will be shown on the list.

External Drive

Current Jobs

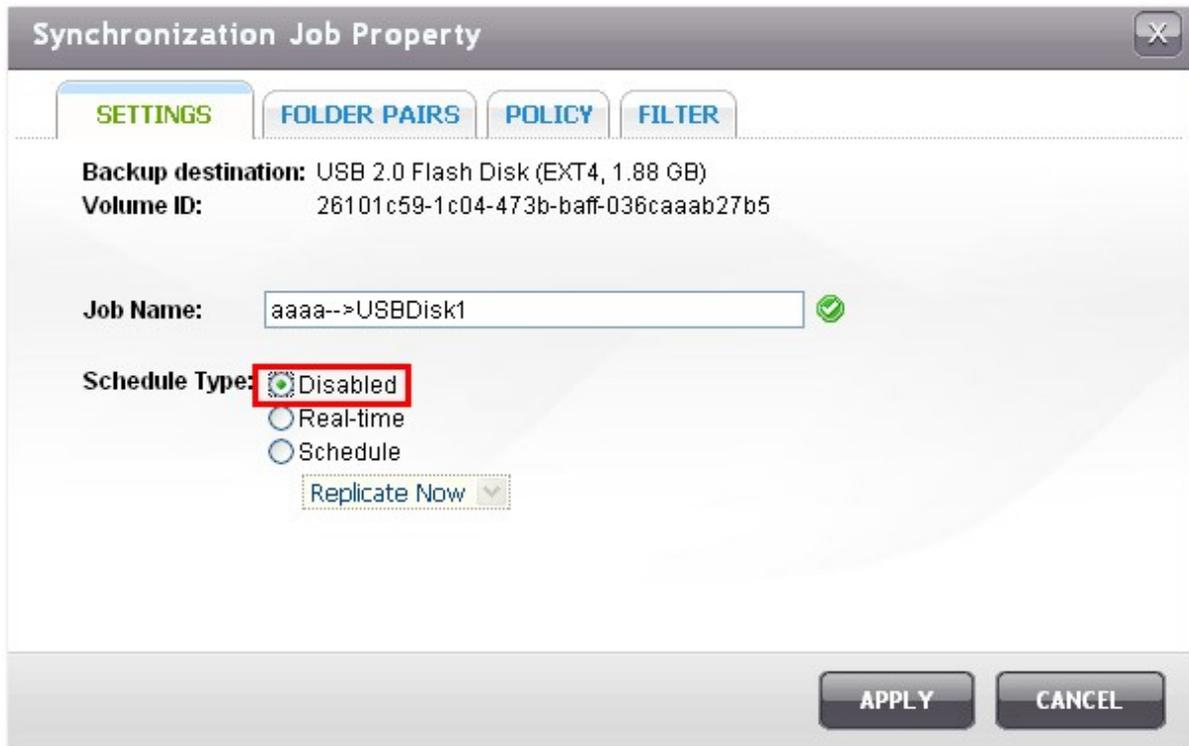
The backup function allows you to replicate the data between the local disk volume and an external storage device. You can create a backup job and map it to a specific disk volume. The external storage device with backup job assigned can always be recognized by the NAS whichever the USB or eSATA interface it is connected to.

Options
Create a new job

	Target Device/Job Name	Status	Action
+	USB 2.0 Flash Disk (EXT4, 1.88 GB) ↳ aaaa-->USBDisk1 (Real-time)	Standby	

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".

Current Jobs

The backup function allows you to replicate the data between the local disk volume and an external storage device. You can create a backup job and map it to a specific disk volume. The external storage device with backup job assigned can always be recognized by the NAS whichever the USB or eSATA interface it is connected to.

[Options](#) [Create a new job](#)

	Target Device/Job Name	Status	Action
+	USB 2.0 Flash Disk (EXT4, 1.88 GB)		

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".

Customize job property

EVENT LOGS | POLICY | FILTER

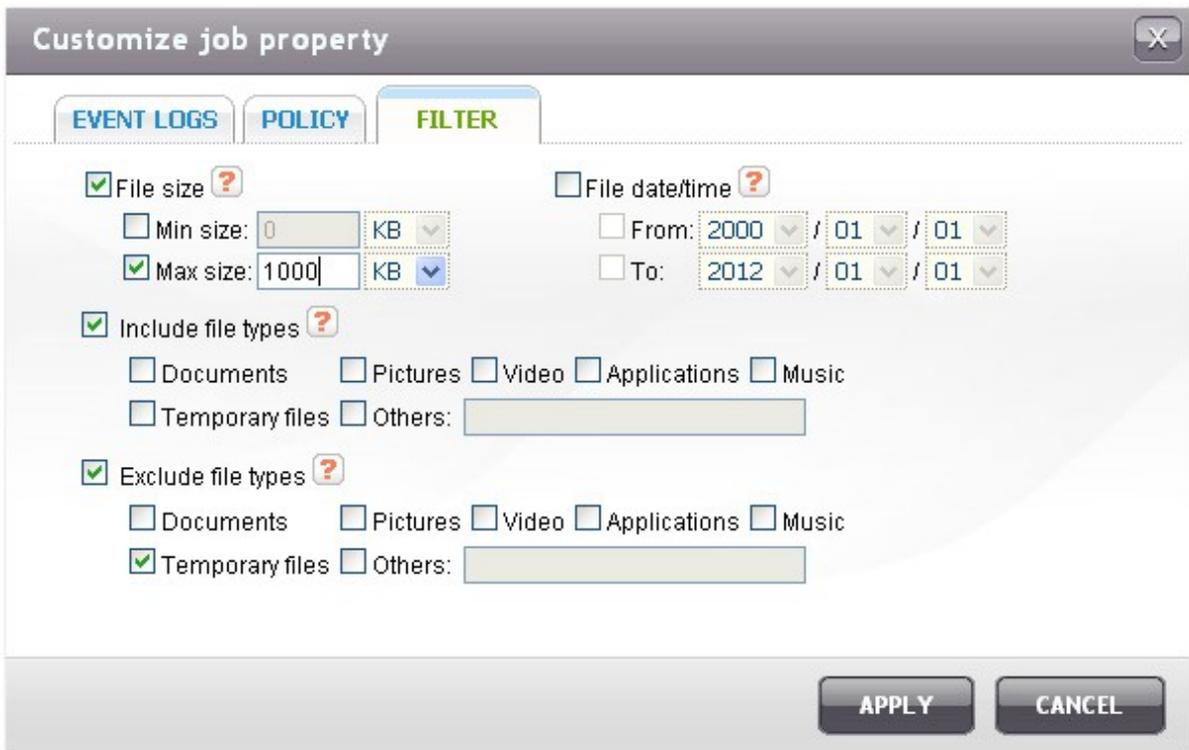
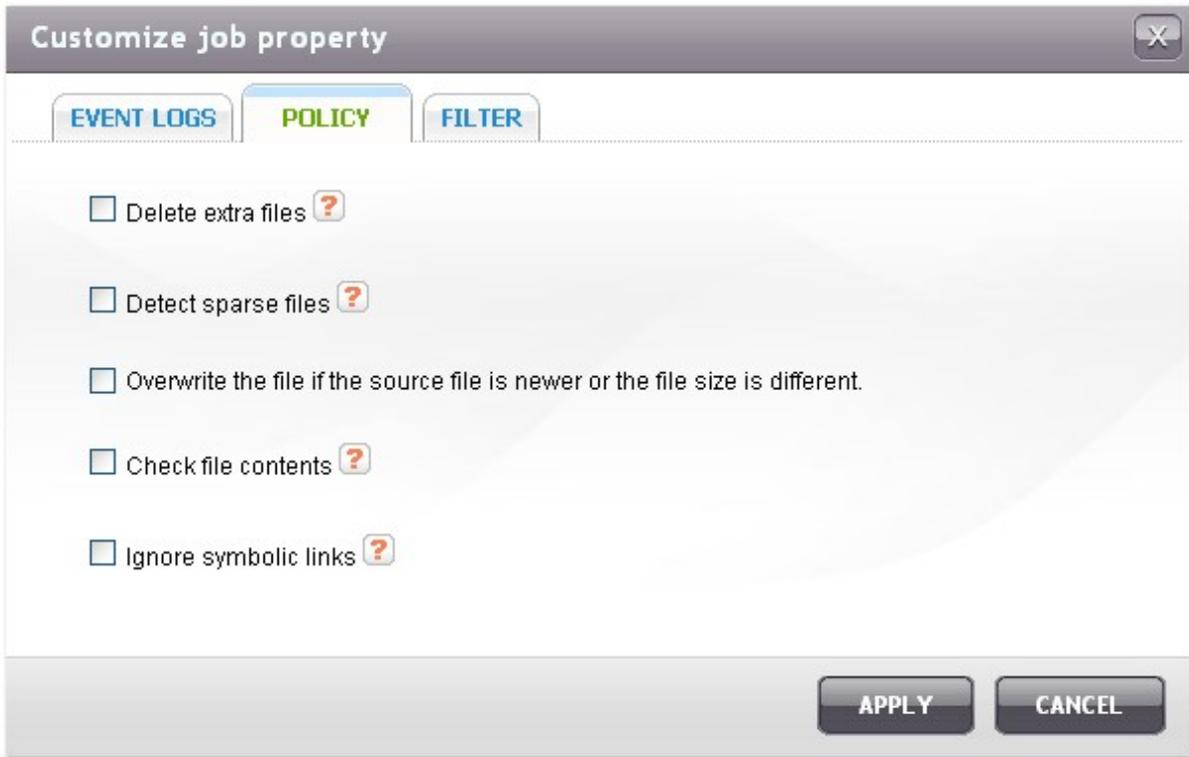
Download Detailed Logs
Maximum Log Size (MB): MB (Max 1GB)
Enable this option to include more information in the log file. You can also specify the maximum file size.

Send an alert email in the following condition(s):
 Synchronization failed
 Synchronization has completed.
Enable this option to allow the system to send an alert email to the system administrator when a synchronization job fails or completes.

Note: The SMTP server must be configured first for alert mail delivery. [Click this to configure the SMTP server](#)

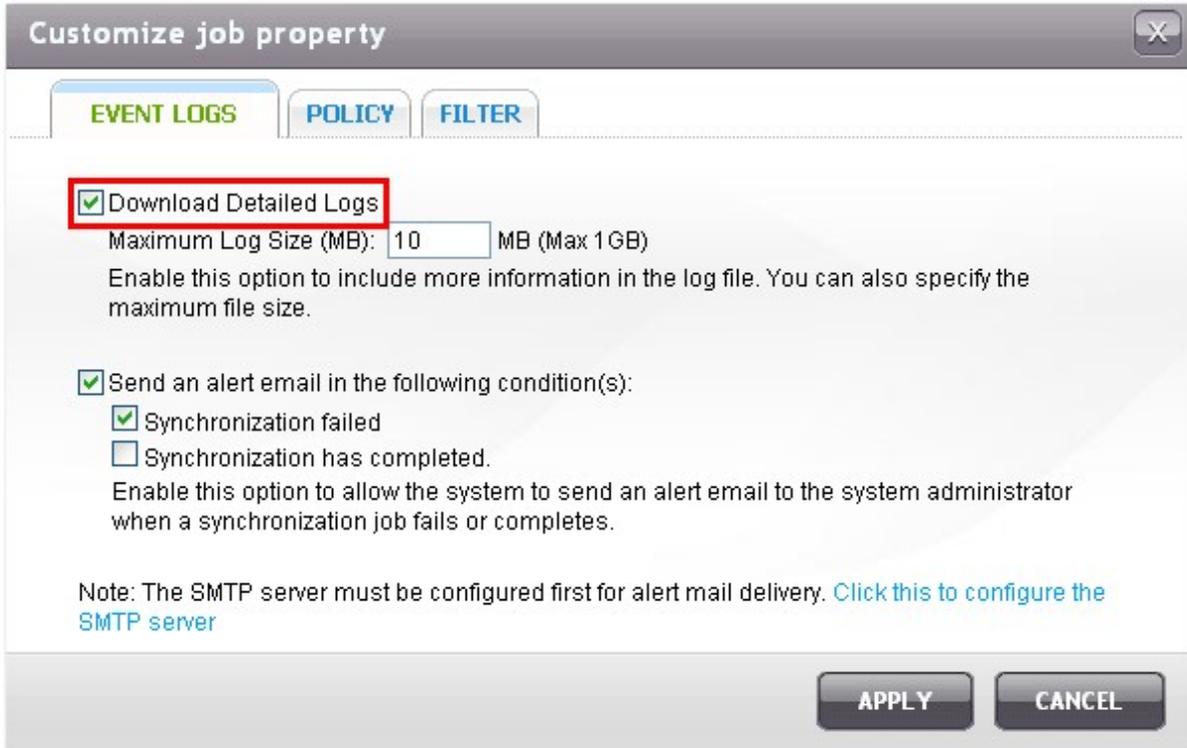
APPLY **CANCEL**

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

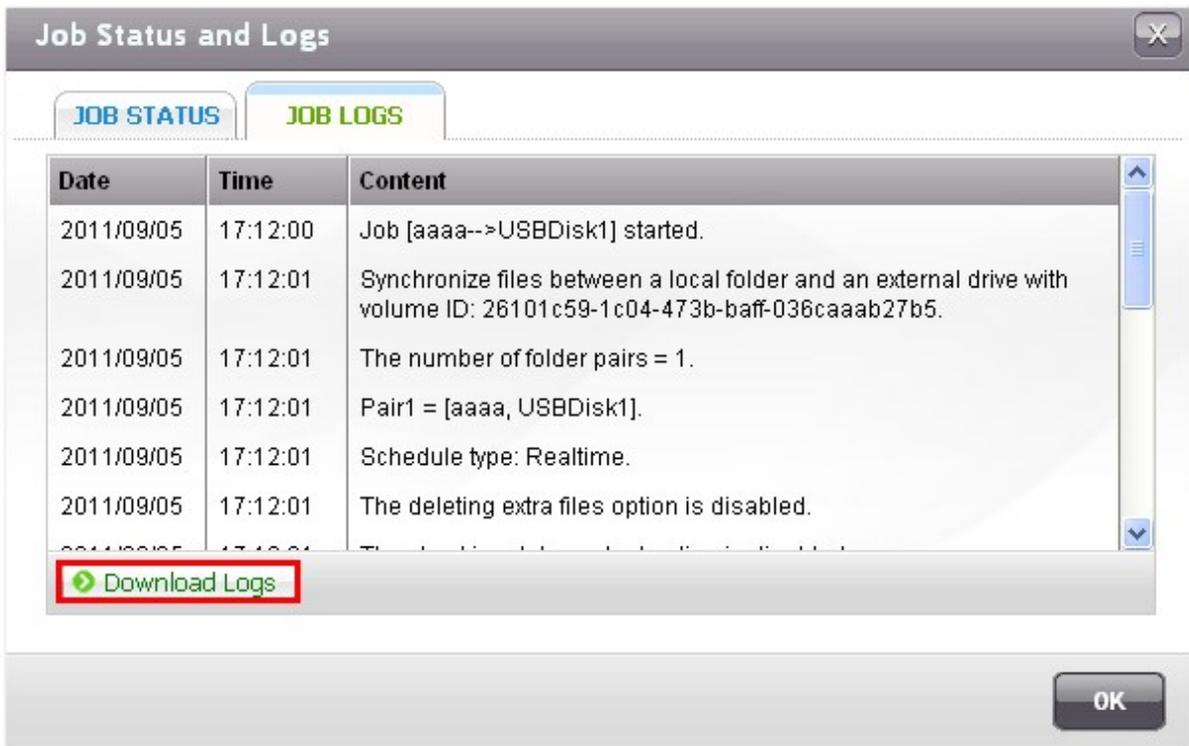
1. To download the logs of a backup job, make sure the option "Download Detailed Logs" in "Options" > "Event Logs" has been enabled.



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.

USB One Touch Copy

Configure the behavior of the USB one touch copy button to back up the data from the front USB drive to the NAS or vice versa.

Enable one touch copy button

Backup direction: The front USB drive --> NAS Backup method: Synchronize

WARNING! 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.

Handle sparse files efficiently

Source folder: → Destination folder: ADD

Source folder	Destination folder	Action
/FrontUSB/Docs	/Multimedia/temp	✕

Unmount the front USB drive manually

Enable alarm buzzer

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^[602]

USB Printer^[612]

UPS Settings^[642]

9.1 External Storage Device

The NAS supports external USB and eSATA storage devices* for backup and data storage. 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".

External Storage Device

External Storage Device

USBDisk1	Manufacturer:	Generic
	Model:	Flash Disk
	Device Type:	USB 2.0
	Total / Free Size:	1.88 GB / 0 MB
	File System:	Unknown
	Status:	Unmounted
	Format As:	EXT4 <input type="button" value="FORMAT NOW"/> Advanced format options
	Eject:	<input type="button" value="DISCONNECT DISK PARTITION"/> <input type="button" value="REMOVE DEVICE"/>

To remove the hardware device, please click [Remove device]. When the system does not show the device anymore, you can remove it safely.

Note: Do NOT unplug the device when it is in use to protect the device.

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.

The screenshot displays the 'External Storage Device' management page. On the left, a list shows 'USBDisk1'. To the right, device details are listed: Manufacturer: Generic, Model: Flash Disk, Device Type: USB 2.0, Total / Free size: 1.88 GB / 0 MB, File System: EXT3, and Status: Locked. A red box highlights the 'ENCRYPTION MANAGEMENT' button next to the status. Below this, there is a 'Format As' dropdown set to 'EXT4', a 'FORMAT NOW' button, and a link for 'Advanced format options'. At the bottom, there are buttons for 'DISCONNECT DISK PARTITION' and 'REMOVE DEVICE', along with an 'Eject:' label.

External Storage Device	
USBDisk1	Manufacturer: Generic
	Model: Flash Disk
	Device Type: USB 2.0
	Total / Free size: 1.88 GB / 0 MB
	File System: EXT3
	Status: Locked ENCRYPTION MANAGEMENT
Format As: EXT4	FORMAT NOW Advanced format options
Eject:	DISCONNECT DISK PARTITION
	REMOVE 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".

The screenshot shows a window titled "Encryption Management" with a close button (X) in the top right corner. On the left side, the QNAP logo and "TURBO NAS" are displayed. The main content area is titled "Encryption Management" in green text. Below the title, it says "Unlock this device by" followed by two radio button options: "Password" (which is selected) and "Key file". Below these options is a password input field with ten black dots. Underneath the password field is a checked checkbox labeled "Save encryption key". At the bottom left of the window, it says "Step 2 of 2". At the bottom right, there are two buttons: "BACK" and "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".

Encryption Management

QNAP
TURBO NAS

Encryption Management

Change encryption key

Old Password:

New Password:

Verify New Password:

Download encryption key file

Password:

Step 2 of 2

BACK **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.

USB Printer

PRINTER | **OPTIONS**

USB Printer

nasPR3

Stop printer sharing and clear print spool

Manufacturer: Hewlett-Packard
Model: HP LaserJet 2200
Status: Ready

Clean up spool space of printer: **CLEAN NOW**

Bonjour printer support

Service Name: nasPR3

APPLY

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.

The screenshot shows a configuration window titled "USB Printer" with two tabs: "PRINTER" and "OPTIONS". The "OPTIONS" tab is active. Under the "Options" section, there are three main fields: "Maximum number of jobs per printer" with a value of 500, "Enter the IP addresses or domain names which are allowed or denied to use the printer service:" with an information icon, and "Access Right" with a dropdown menu set to "No limit". Below these is a large empty text area for IP addresses. An "APPLY" button is located at the bottom right.

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.

Enter the IP addresses or domain names which are allowed or denied to use the printer service: ⓘ

Access Right: 

- No limit
- Allow printing
- Deny printing

*

APPLY

Pause, resume, or delete printer jobs

You can pause or cancel ongoing or pending jobs, resume paused jobs, or delete completed or pending jobs.

Users:  

Users	Source IP	File name	Status	Action
admin	10.8.12.43	--	completed (30/Nov/2010:15:58:12)	

Total: 1 | Display entries per page. 

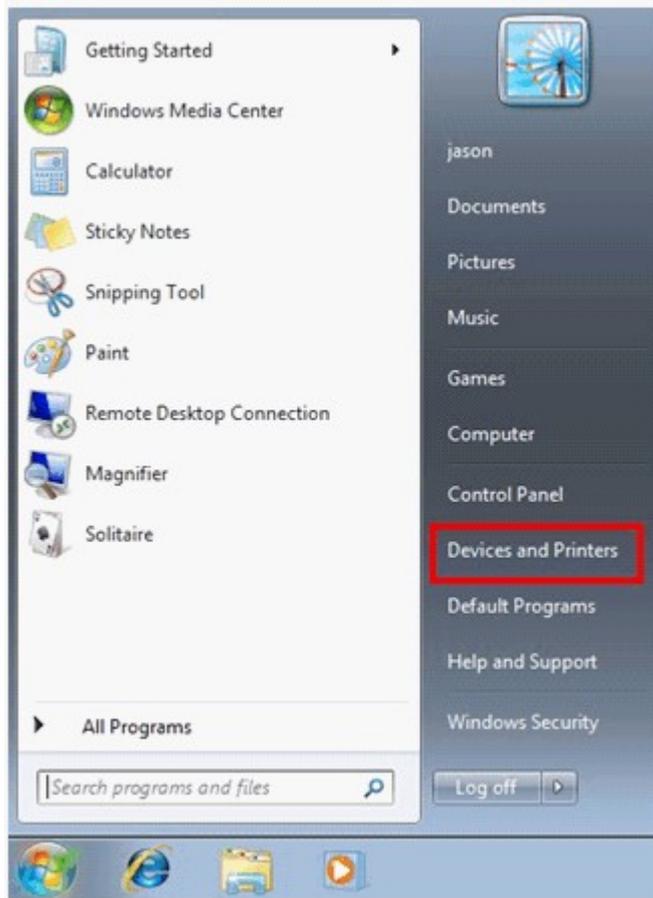
Note: Do NOT restart the NAS or update the system firmware when printing is in process or there are queued jobs. Otherwise all the queued jobs will be cancelled and removed.

9.2.1 Windows 7, Vista Users

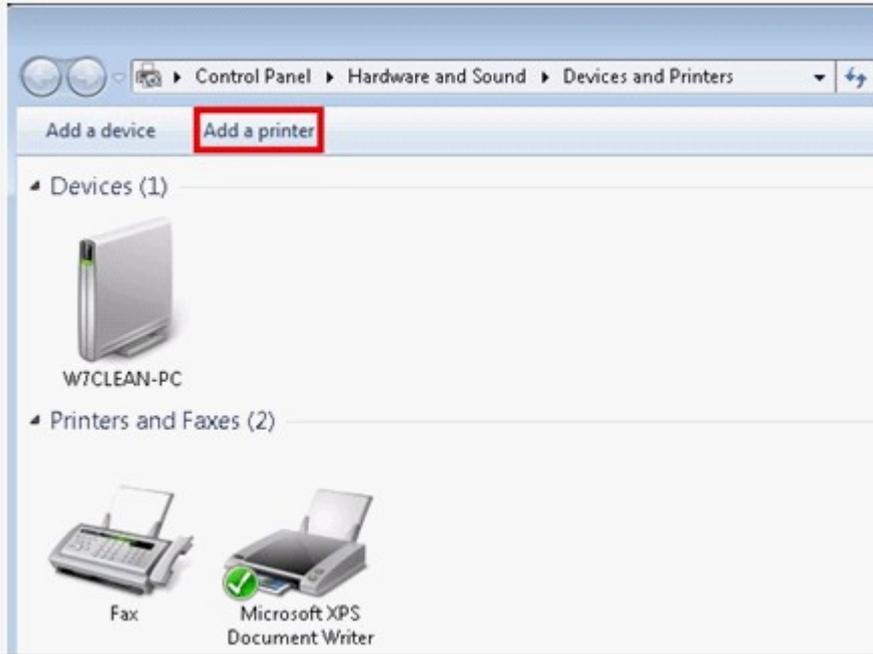
The following description applies to Windows 7.

Follow the steps below to set up your printer connection.

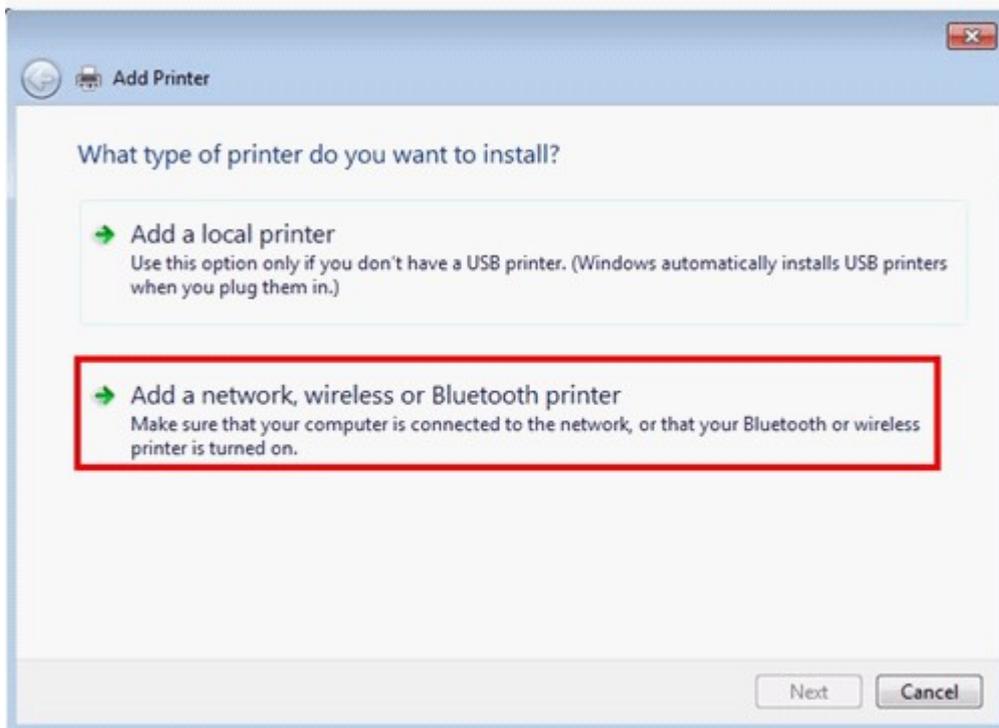
1. Go to Devices and Printers.



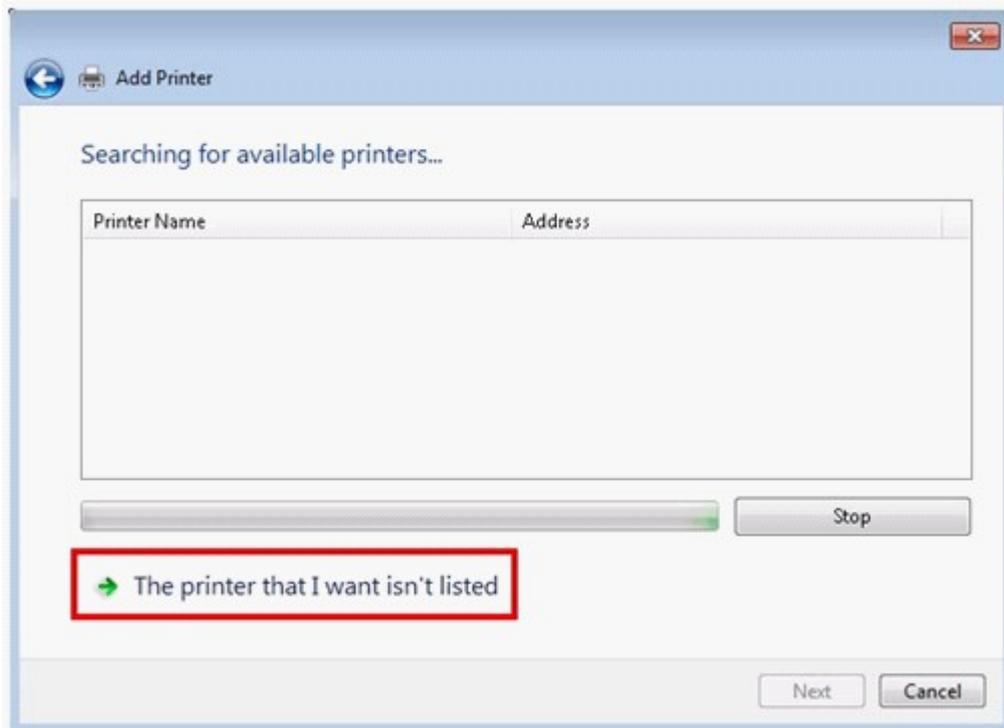
2. Click "Add a printer".



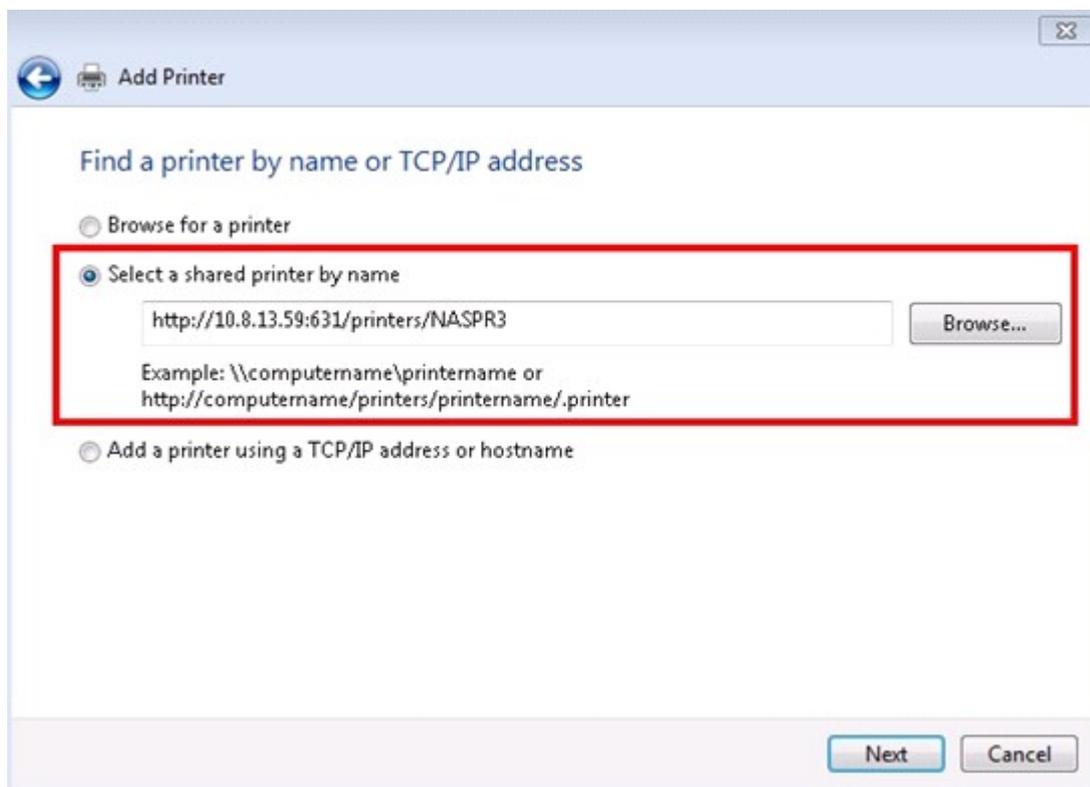
3. In the Add printer wizard, click "Add a network, wireless or Bluetooth printer".



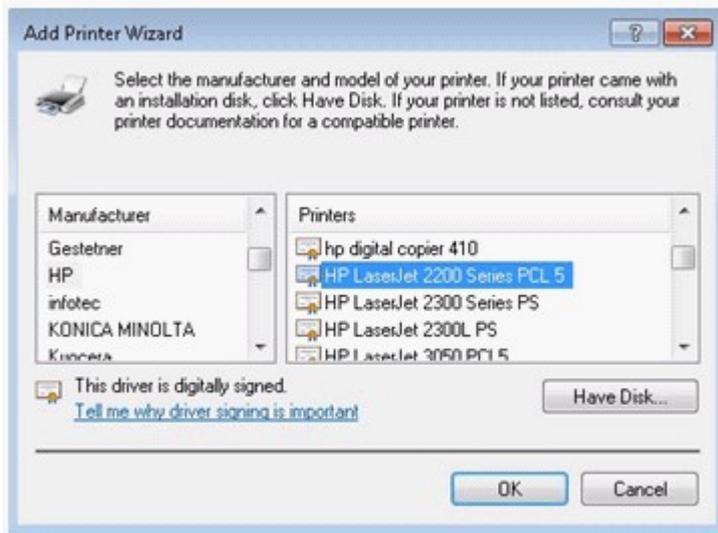
4. While Windows is searching for available network printers, click "The printer that I want isn't listed".



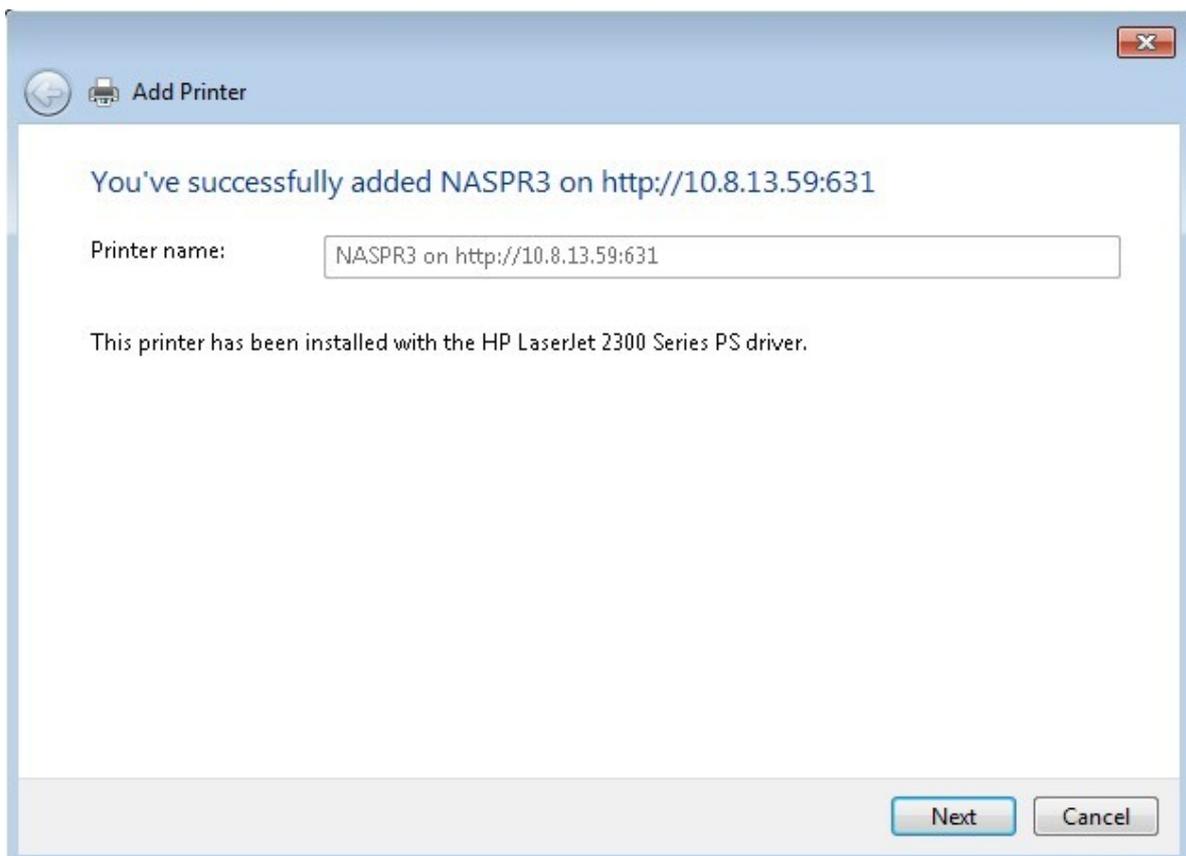
5. Click "Select a shared printer by name", and then enter the address of the network printer. The address is in the following format – `http://NAS_IP:631/printers/ServernamePR`, where the NAS_IP can also be a domain name address if you want to print remotely. For example, `http://10.8.13.59:631/printers/NASPR3`



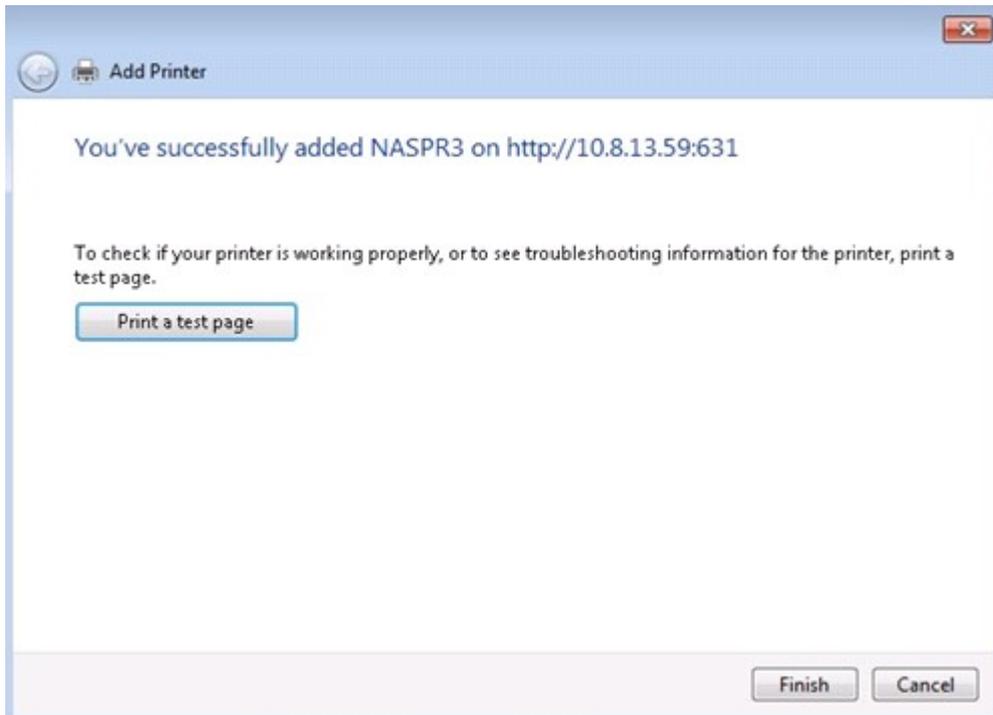
- The wizard will prompt you for the correct printer driver. You may also download the latest printer driver from the manufacturer's website if it is not built-into Windows operating system.



- 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.

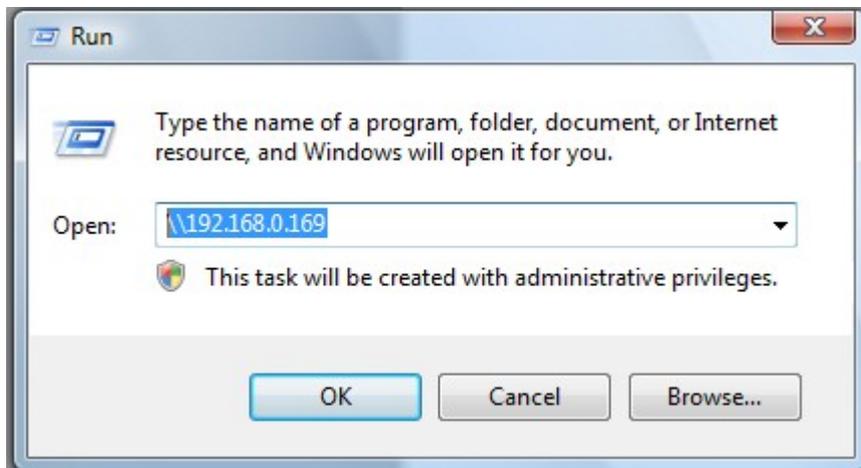


9. The new network printer is now available for printing.

The following description applies to Windows 7 and Vista OS.

Follow the steps below to set up your printer connection.

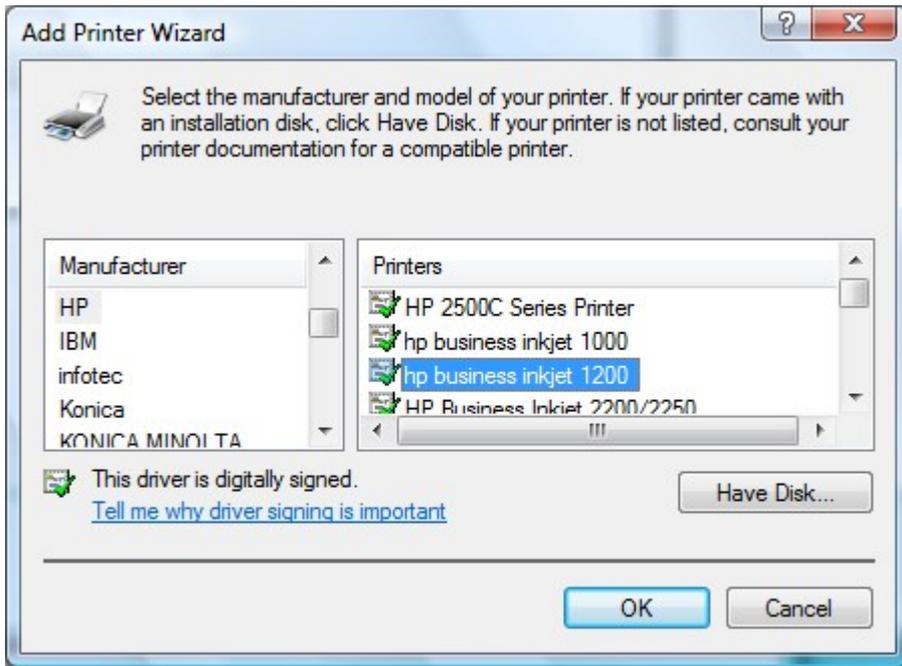
1. On the Run menu, enter \\NAS IP.



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

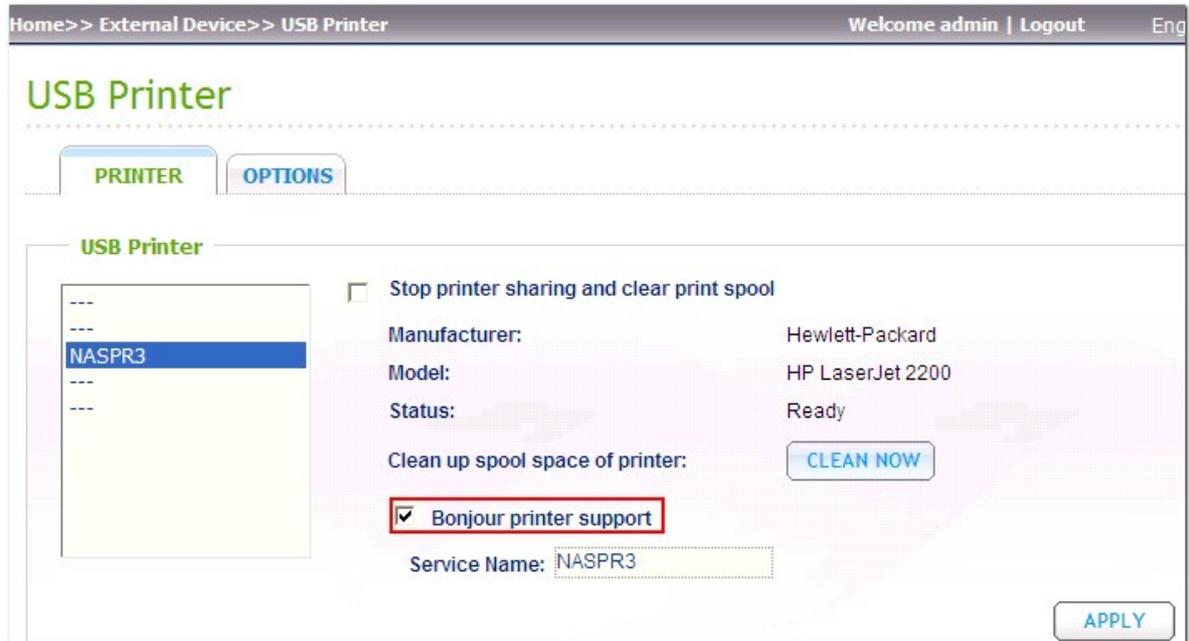
The following configuration method has been verified on Windows XP only:

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.

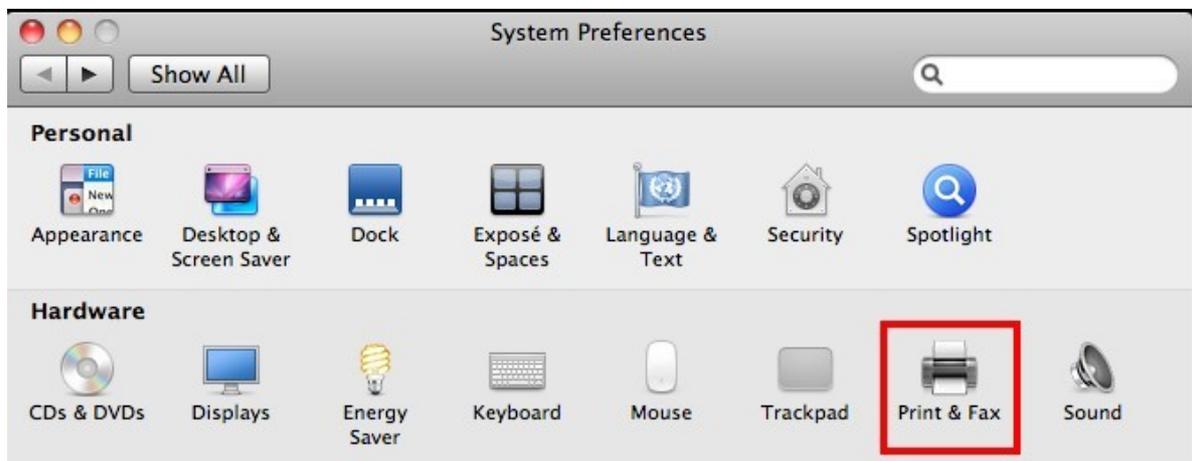
9.2.3 Mac OS 10.6

If you are using Mac OS 10.6, follow the steps below to configure the printer function of the NAS.

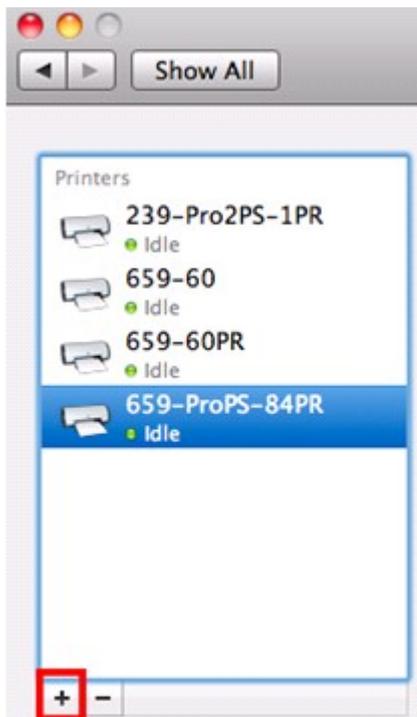
1. First make sure the Bonjour printer support is enabled on the NAS in "External Device" > "USB Printer". You may change the Service Name to better represent the printer.



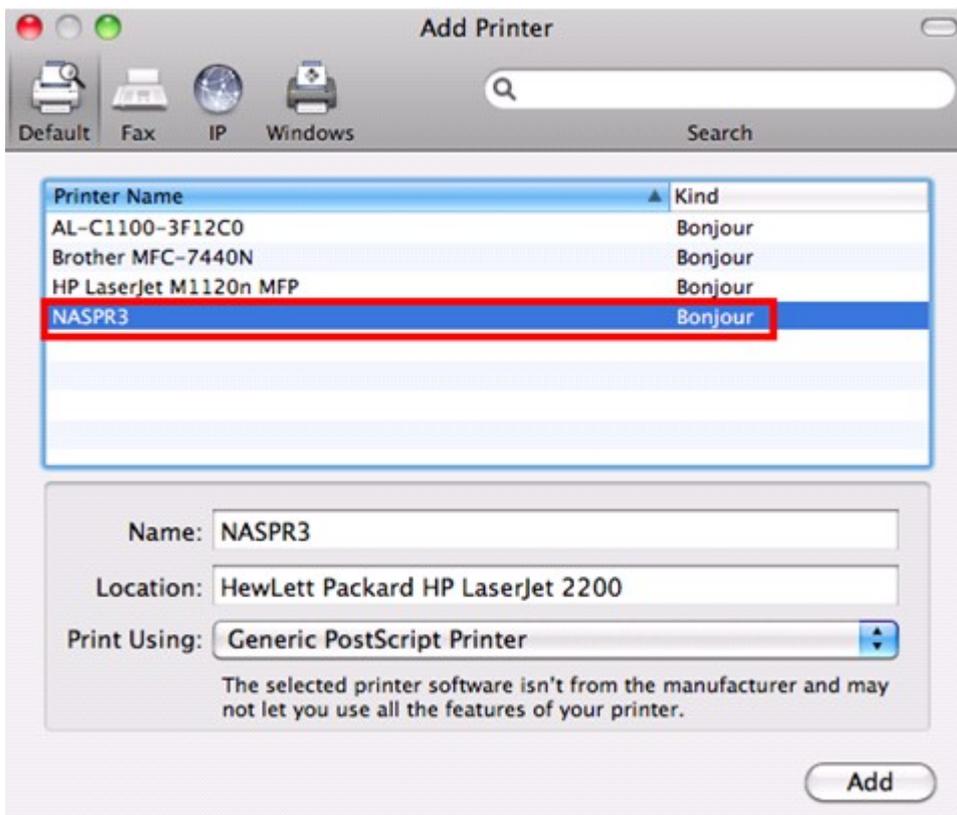
2. On your Mac, go to "System Preferences", and then click "Print & Fax".



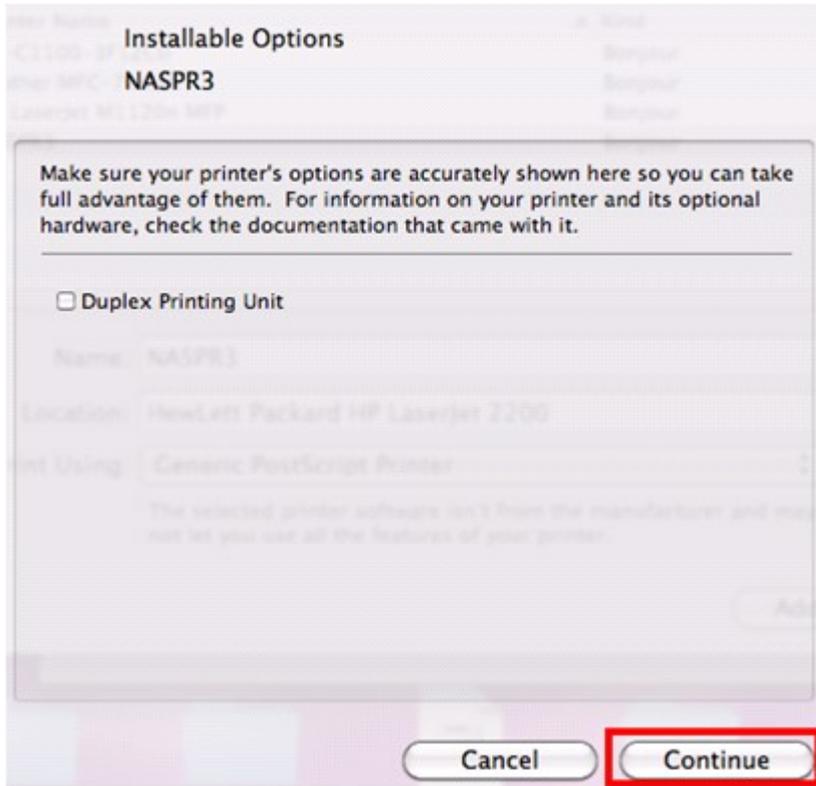
3. In the Print & Fax window, click + to add a printer.



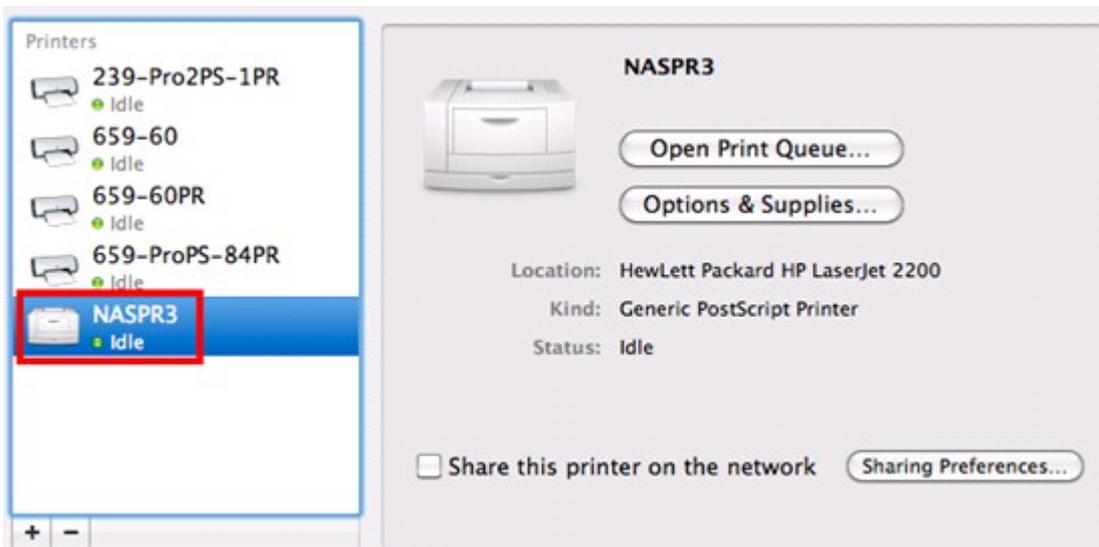
4. The USB network printer will be listed via Bonjour. Select the default printer driver or you may download and install the latest one from the printer manufacturer's website. Click "Add" to add this printer.



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.

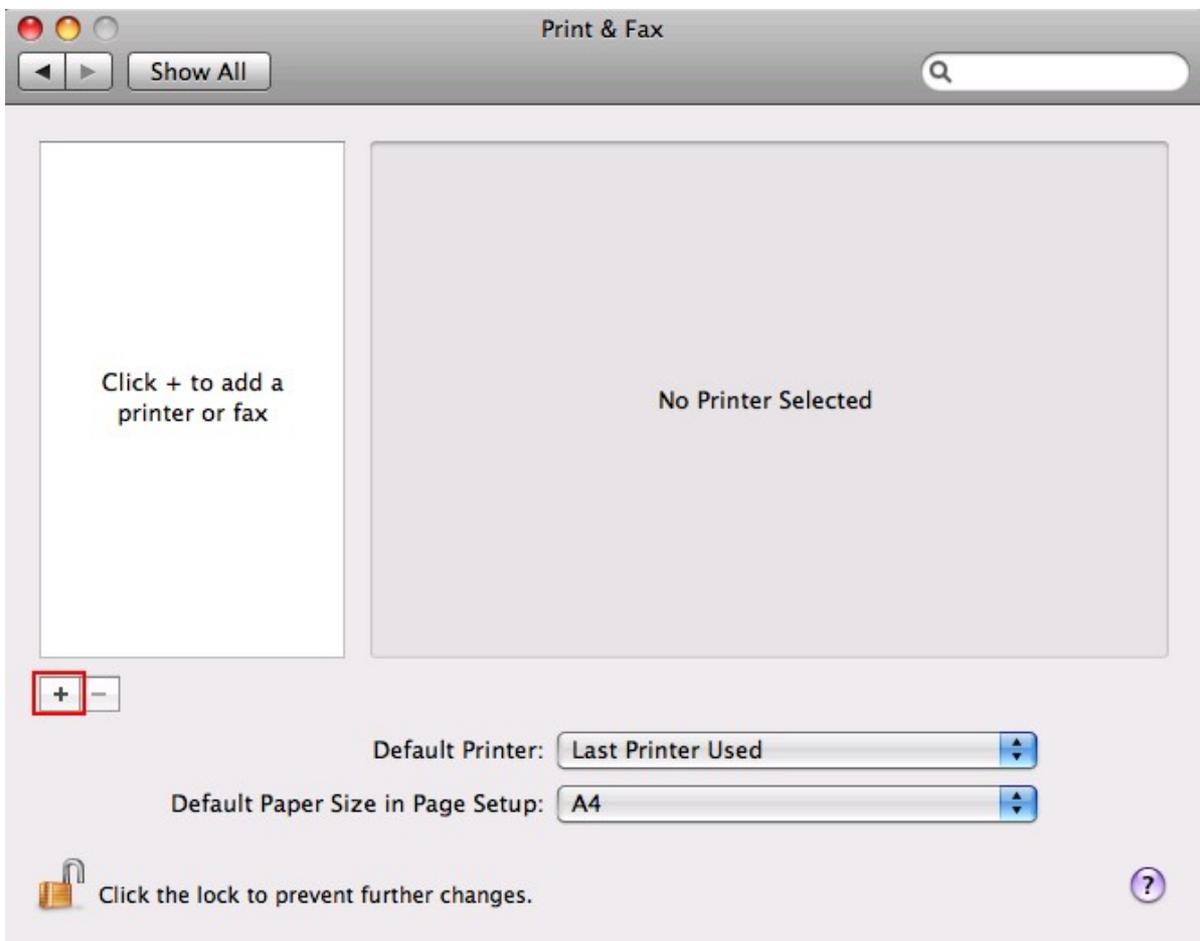
1. Make sure your printer is connected to the NAS and the printer information is displayed correctly on the "USB Printer" page.
2. Go to "Network Services" > "Microsoft Networking". Enter a workgroup name for the NAS. You will need this information later.

The screenshot shows a web interface for configuring Microsoft Networking. The breadcrumb trail is "Home >> Network Services >> Microsoft Networking". The user is logged in as "admin" and the language is set to "English". The page title is "Microsoft Networking". There are two tabs: "MICROSOFT NETWORKING" (selected) and "ADVANCED OPTIONS". Under the "Microsoft Networking" section, the "Enable file service for Microsoft networking" checkbox is checked. The "Server Description (Optional)" field contains "NAS Server". The "Workgroup" field is highlighted with a red box and contains "Workgroup". There are three radio button options: "Standalone Server" (selected), "AD Domain Member (To enable Domain Security, please click here.)", and "LDAP Domain Authentication (To enable Domain Security, please click here.)". The "Current Samba ID" is "S-1-5-21-325120726-1639715159-2191483818". An "APPLY" button is located at the bottom right.

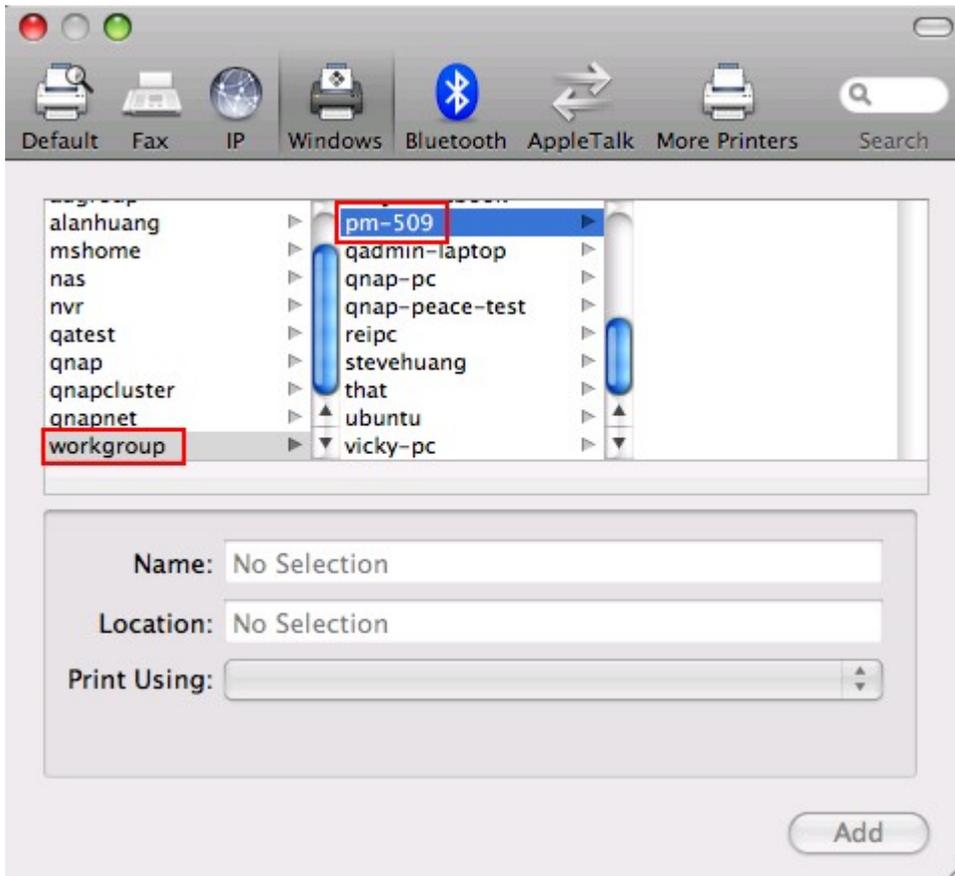
3. Go to "Print & Fax" on your Mac.



4. Click + to add a printer.



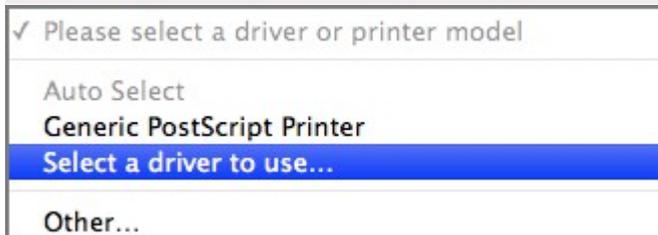
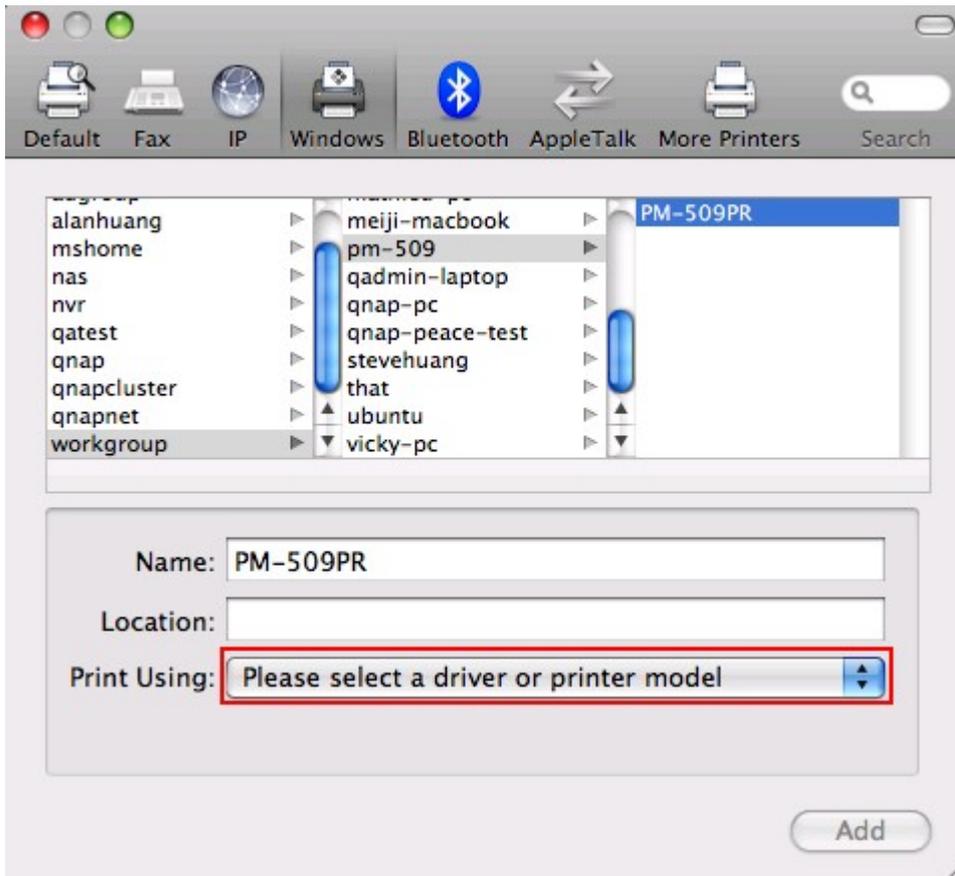
5. Select the NAS workgroup and find the printer name.



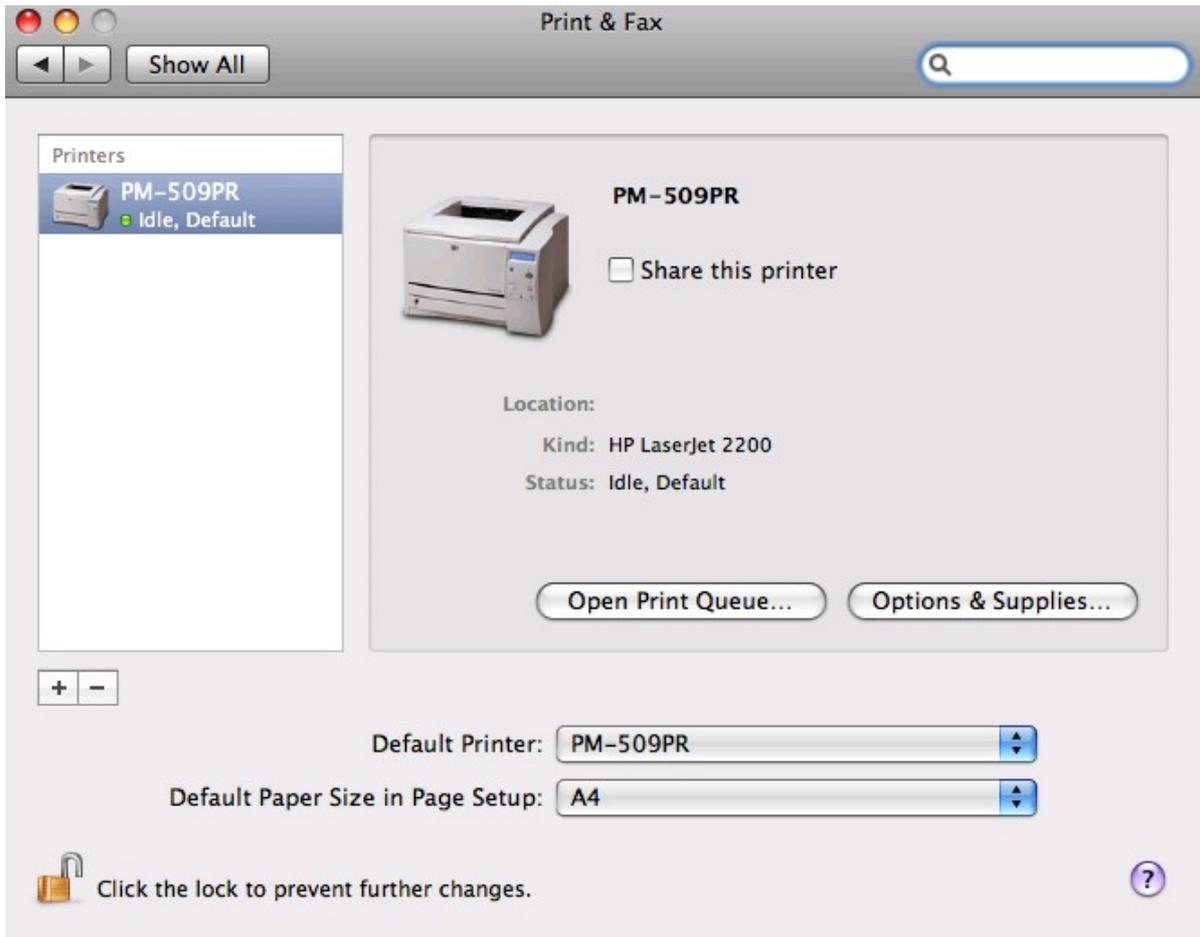
6. Enter the username and password to login the printer server on the NAS.



7. Select the printer driver.



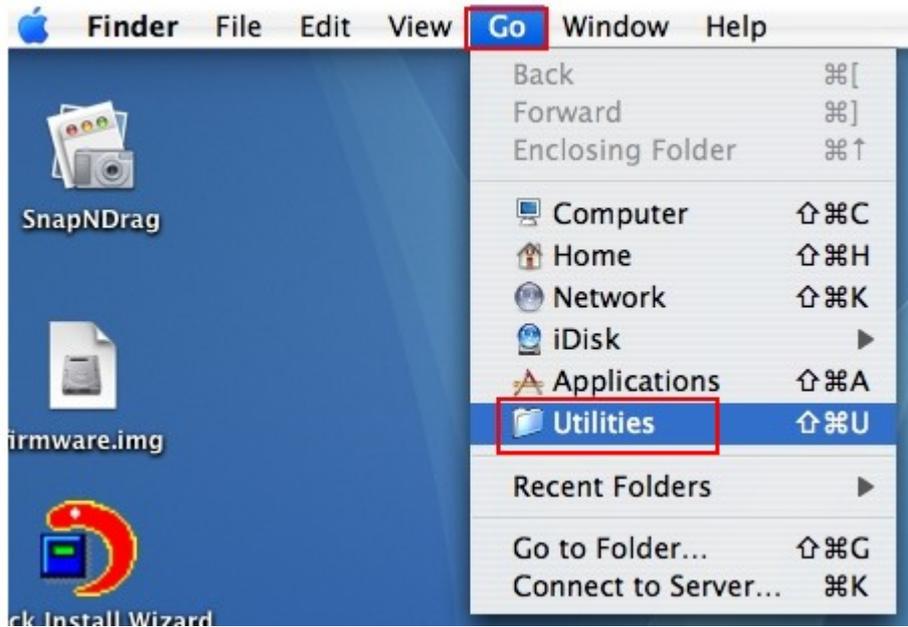
8. After installing the printer driver correctly, you can start to use the printer.



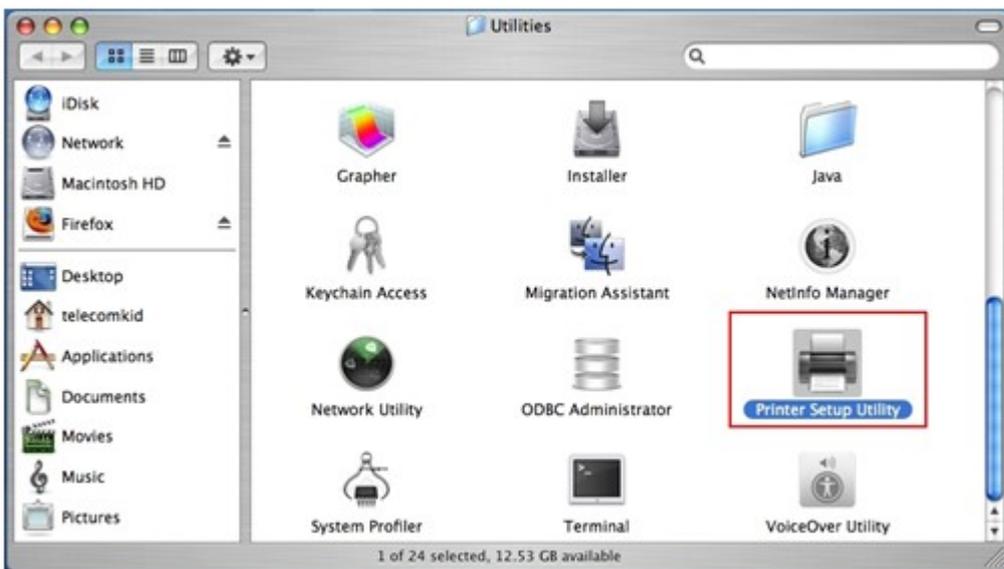
9.2.5 Mac OS 10.4

If you are using Mac OS 10.4, follow the steps below to configure the printer function of the NAS.

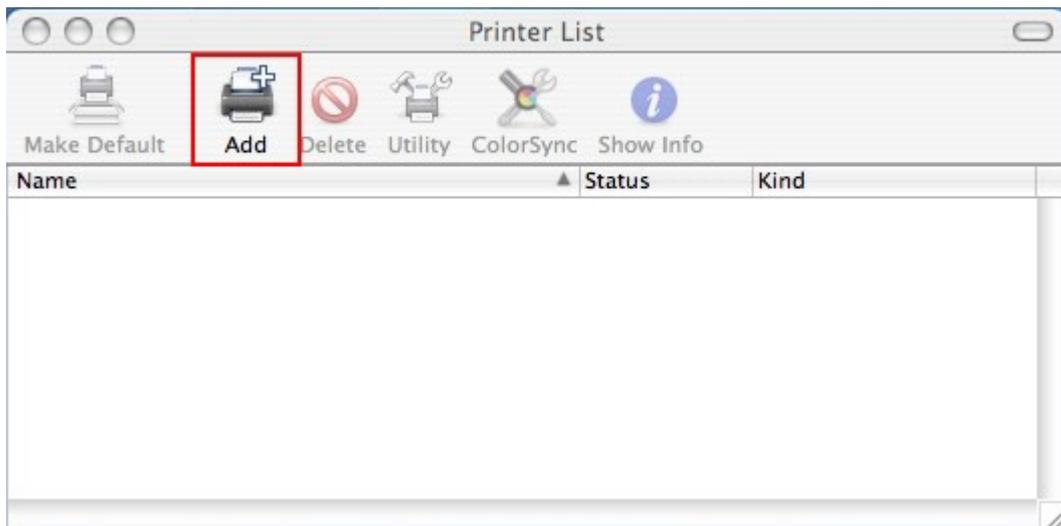
1. On the toolbar, click "Go/Utilities".



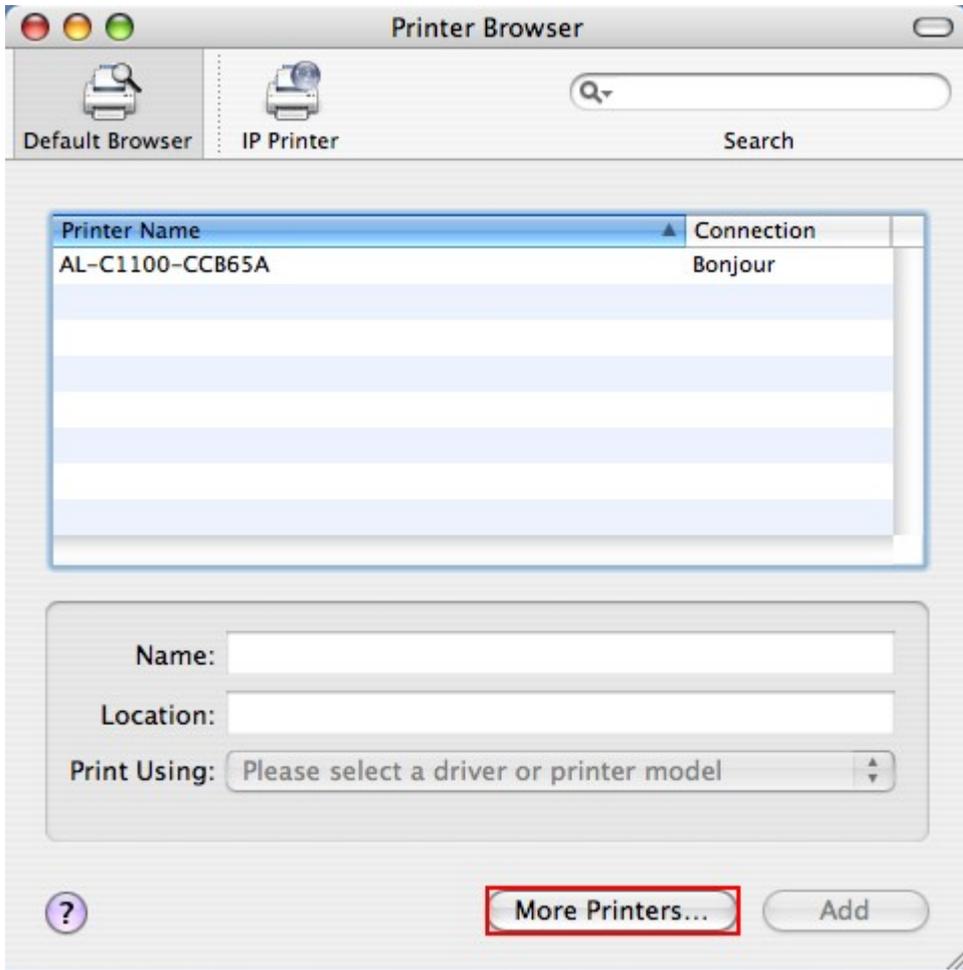
2. Click "Printer Setup Utility".



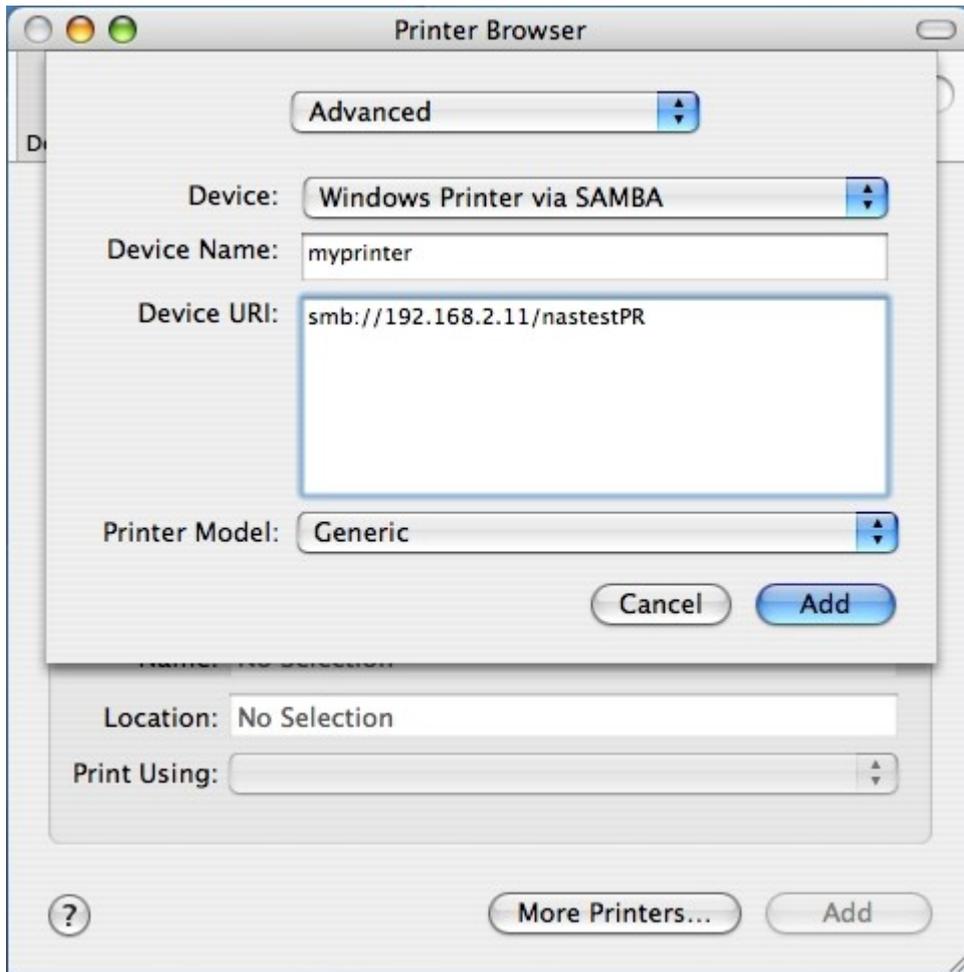
3. Click "Add".



4. Press and hold the "alt" key  on the keyboard and click "More Printers" concurrently.

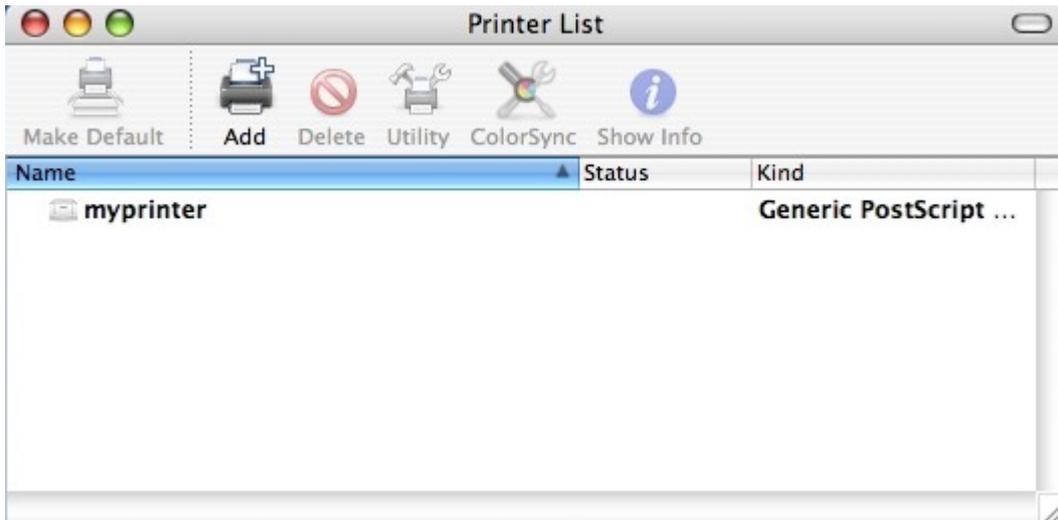


5. In the pop up window:
 - a. Select "Advanced"*.
 - b. Select "Windows Printer with SAMBA".
 - c. Enter the printer name.
 - d. Enter the printer URI, the format is smb://NAS IP/printer name. The printer name is found on the "Device Configuration" > "USB Printer page".
 - e. Select "Generic" for Printer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

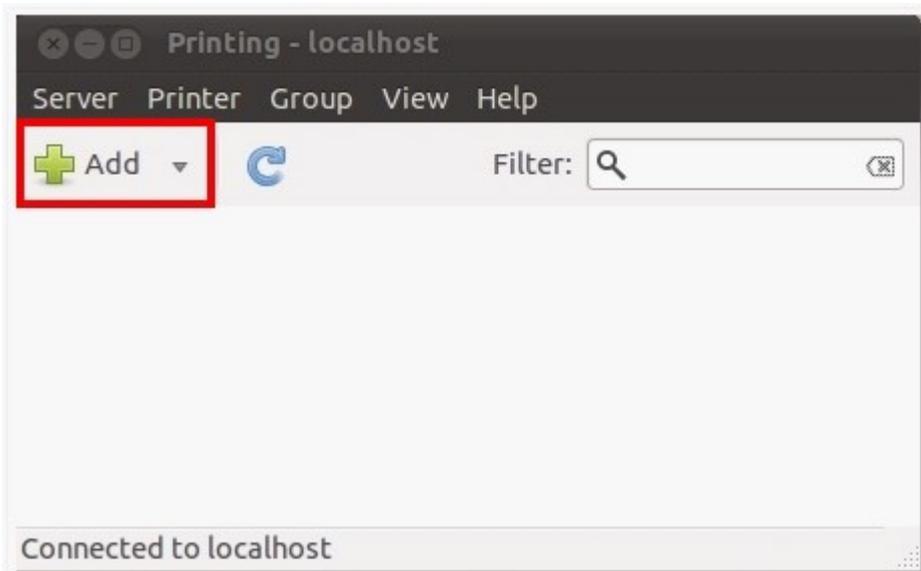
9.2.6 Linux (Ubuntu 10.10)

If you are using Linux (Ubuntu 10.10), follow the steps below to configure the printer function of the NAS.

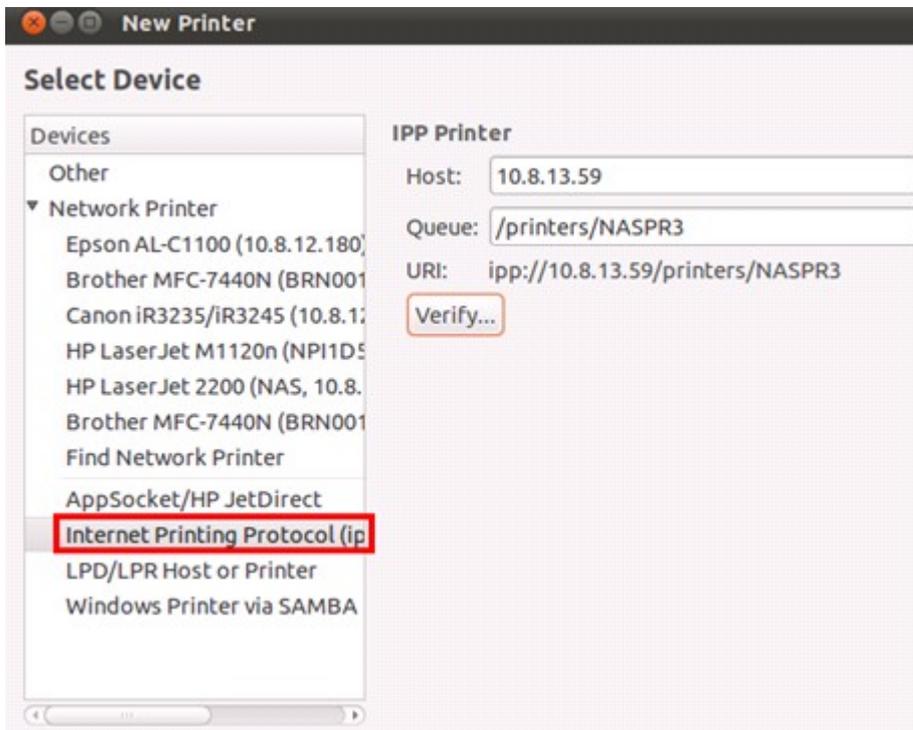
1. Click the "System" tab, choose "Administration". Then select "Printing".



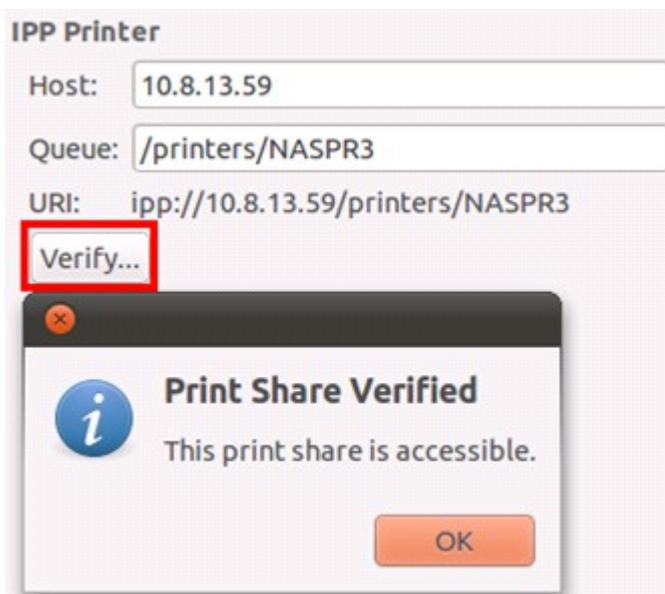
2. Click "Add" to add a printer.



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".



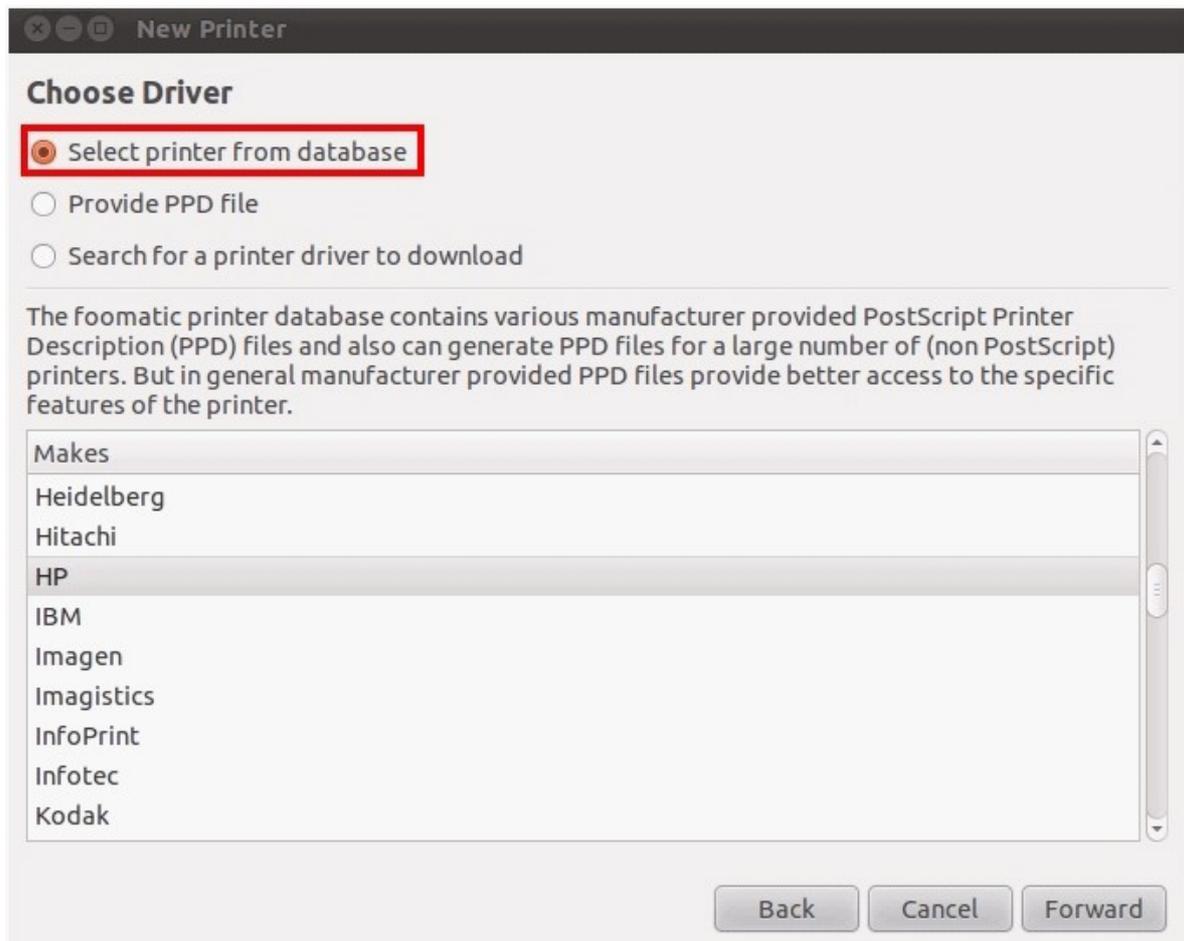
4. Before you continue, you may click "Verify" to test the printer connection.



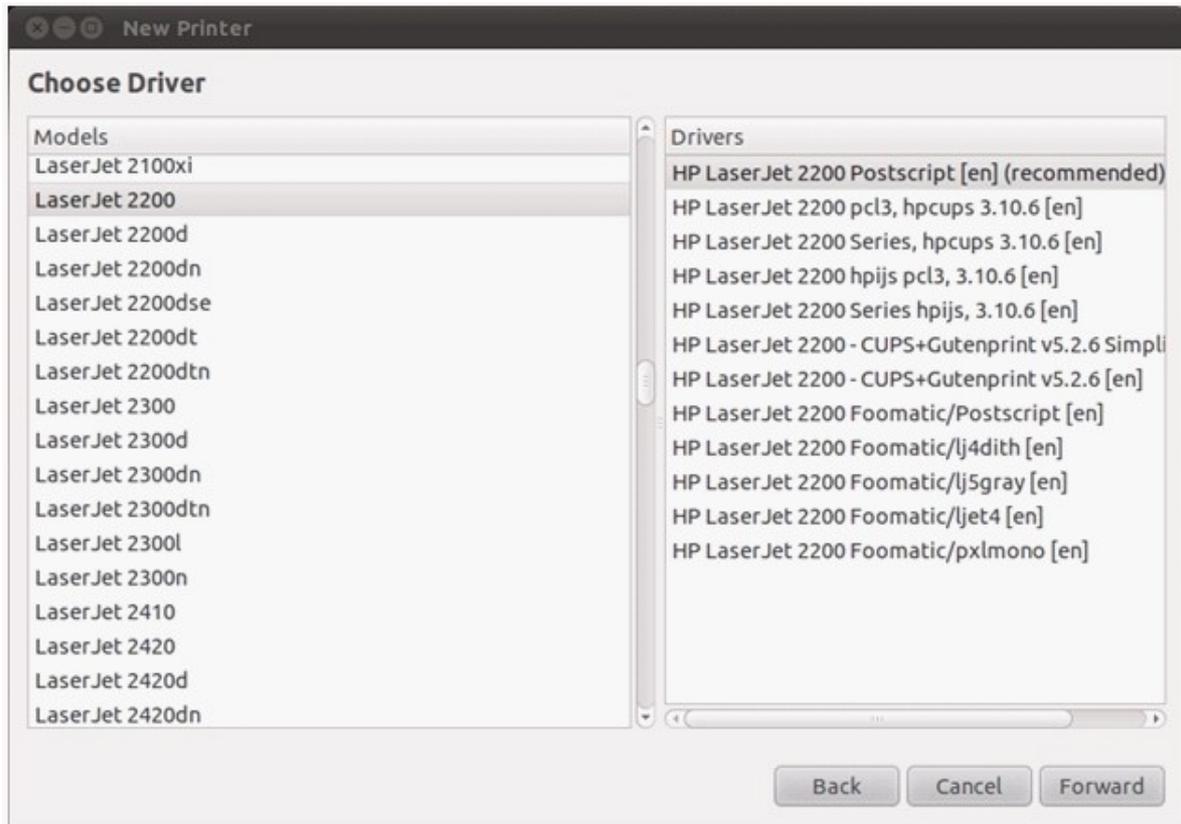
5. The operating system starts to search for the possible driver list.



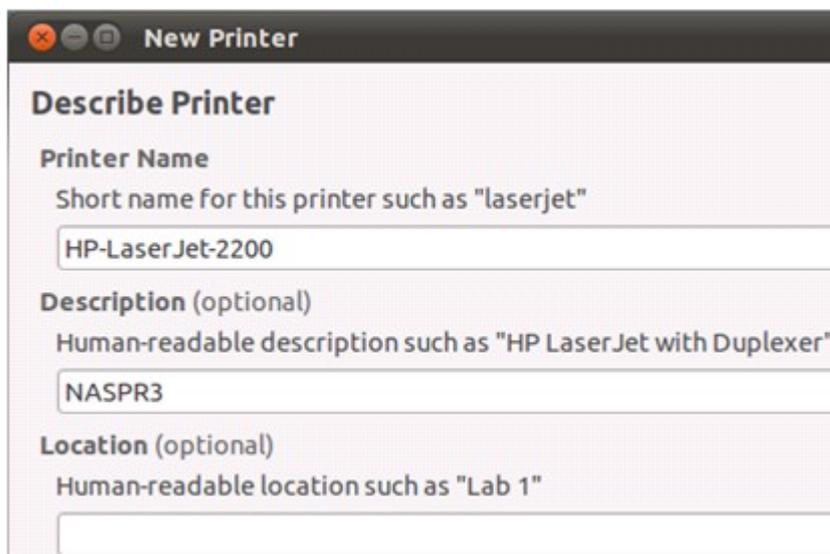
6. Select the printer driver from the built-in database, or search online.



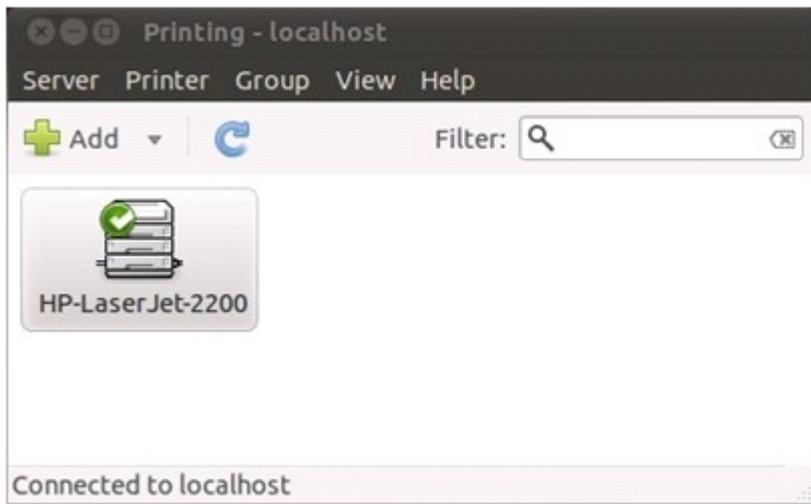
7. Choose the correct printer model and driver. Depending on the printer, some additional printer options may be available in the next step.



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.

UPS Settings

UPS Settings

Enable UPS support

After the AC power fails for minute(s), turn off the server.

After the AC power fails for minute(s), the system will stop all services. The system will restart automatically when the power restores.

Protocol: ▾

IP address of network UPS server:

UPS Information

UPS brand:	--
UPS model:	--
AC power status:	--
Battery capacity:	--
Estimated protection time:	--

[APPLY](#)

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".

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".

MyCloudNAS Wizard

Enter your MyCloudNAS name

Enter a name for your NAS for remote access from the Internet.

http://test123 MyCloudNAS.com

Step 2 of 6

- 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

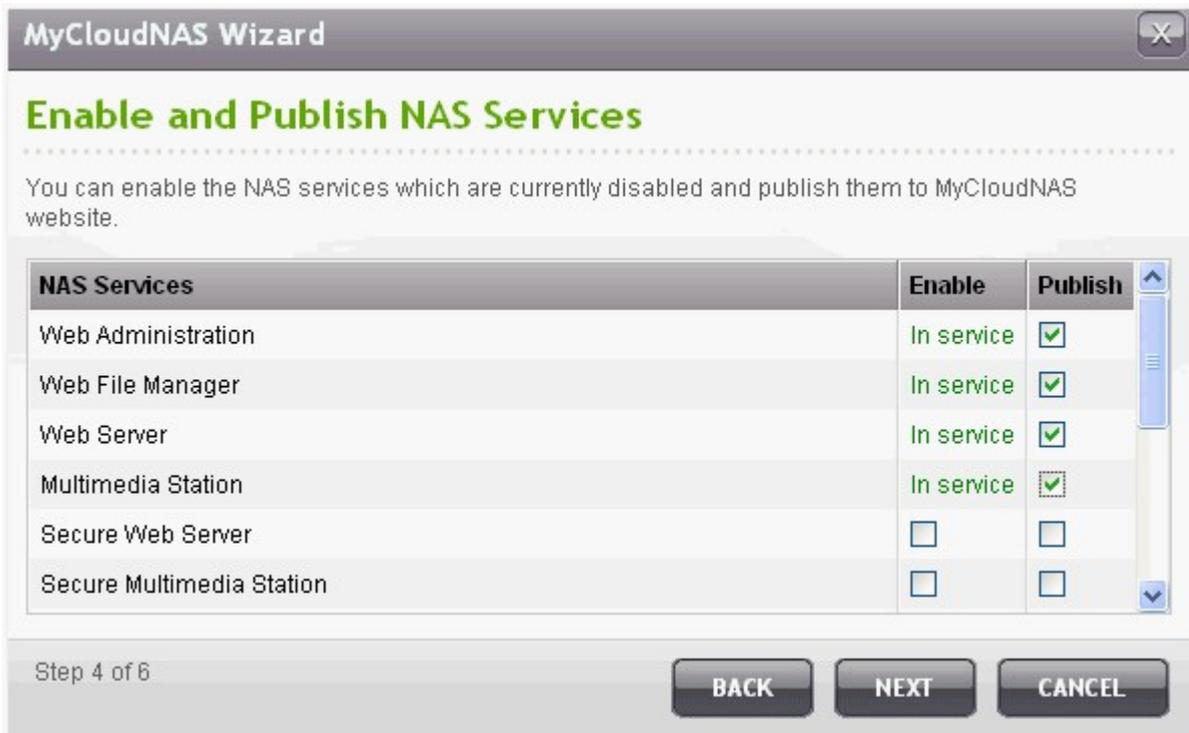


4. Publish NAS services.

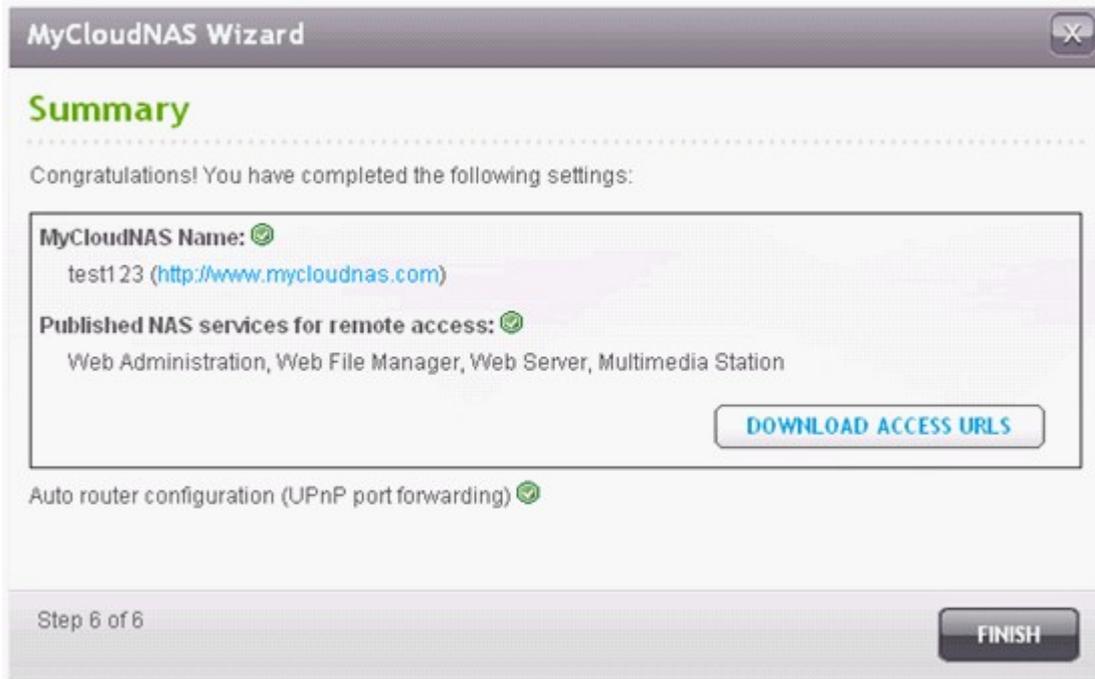
The NAS services which use the ports opened in the previous step will be shown. You can enable the services which are currently disabled and publish the web-based NAS services such as web administration, Web Server, Multimedia Server, and Web File Manager to <http://www.mycloudnas.com>. Click "Next".

By enabling the NAS services in this step, they are opened for remote access even if they were not published.

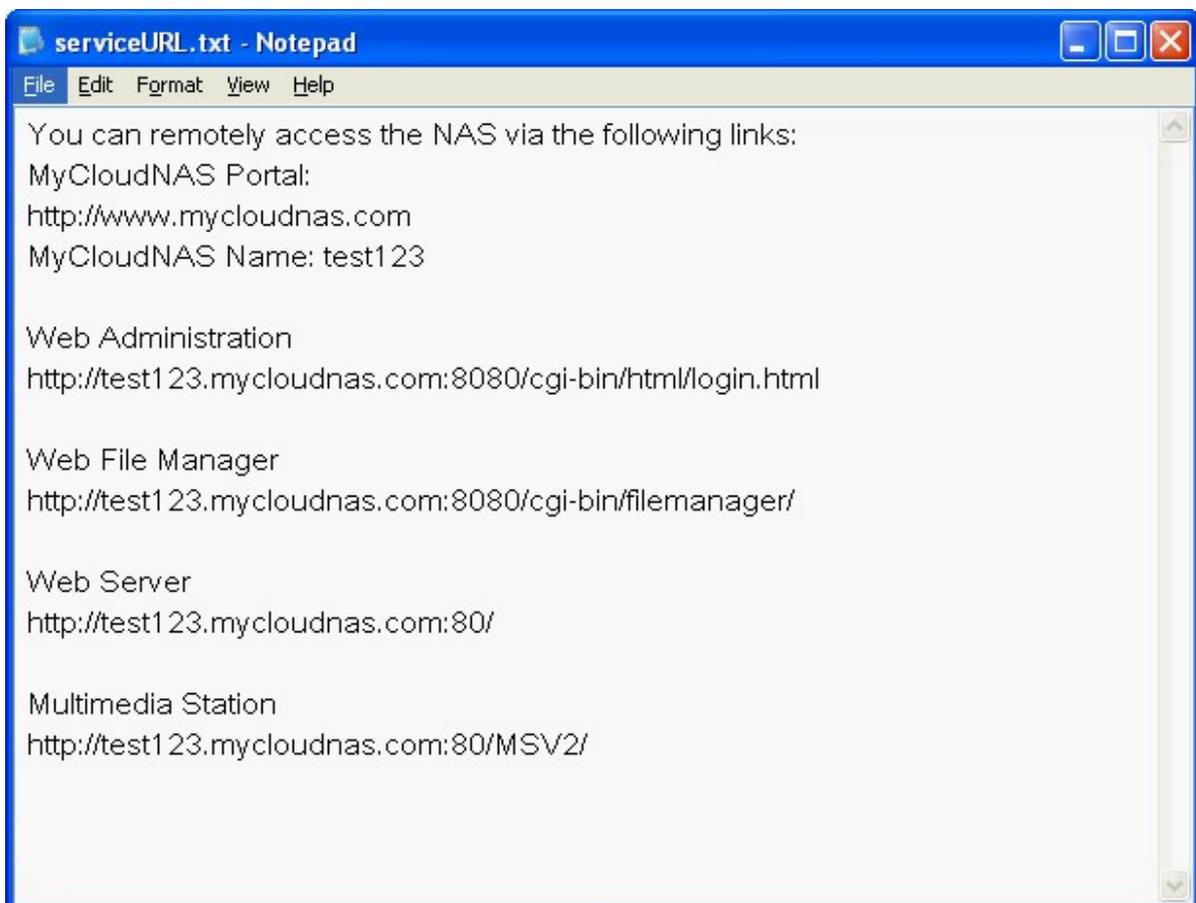
The NAS services can be published in private to allow only the users with the MyCloudNAS Access Code to view the private services on MyCloudNAS website. To use this feature, go to "MyCloudNAS Service" > "Configure MyCloudNAS" > "Publish Services".



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.



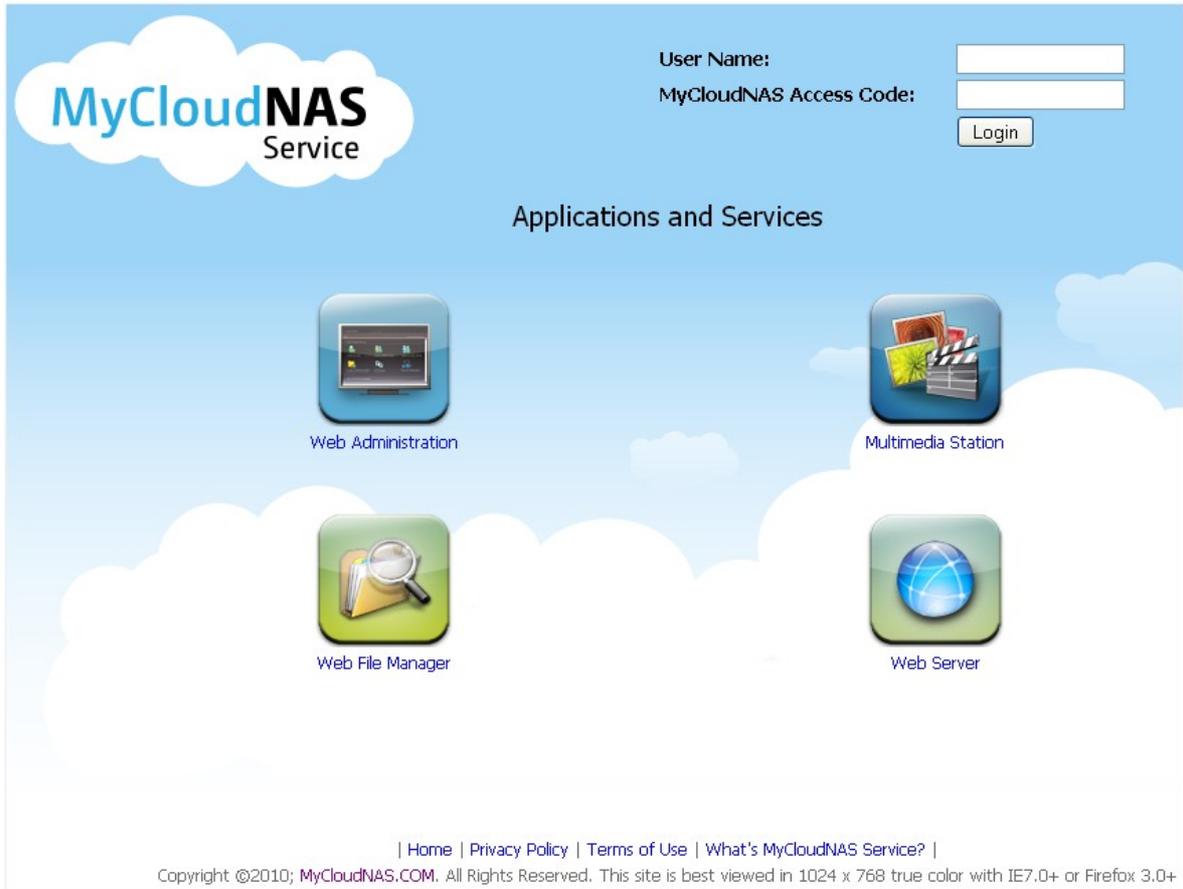
Copy the URLs and access the NAS services by the web browser.



- 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 username 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".

User Name:	<input type="text" value="admin"/>
MyCloudNAS Access Code:	<input type="password" value="••••••••••"/>
	<input type="button" value="Login"/>

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.

The screenshot displays the MyCloudNAS Service interface. At the top left is the logo "MyCloudNAS Service" inside a cloud shape. On the top right, the login status is shown: "User Name: admin" (in a text box), "MyCloudNAS Access Code: passed" (in a text box), and a "Logout" button. Below this is the heading "Applications and Services". There are eight application icons arranged in two rows of four. The first row includes "Web Administration" (laptop icon), "Secure Web Administration" (laptop with lock icon), "Multimedia Station" (clapperboard icon), and "Secure Multimedia Station" (clapperboard with lock icon). The second row includes "Web File Manager" (folder with magnifying glass icon), "Secure Web File Manager" (folder with magnifying glass and lock icon), "Web Server" (globe icon), and "Secure Web Server" (globe with lock icon).

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.

Home >> MyCloudNAS Service >> Configure MyCloudNAS Welcome admin | Logout English

Configure MyCloudNAS

CONFIGURE MYCLOUDNAS | **PUBLISH SERVICES**

Configure MyCloudNAS Name

After enabling this service, you can connect to the NAS by your desired host name.

Enable MyCloudNAS Service

MyCloudNAS Name:

Check the external IP address automatically:

[Click here to launch MyCloudNAS Wizard.](#)

Recent Update Result

Current MyCloudNAS Name:	http://test.mycloudnas.com
Current WAN IP:	219.85.63.13
Last Check Time:	2010/11/30 16:23:22
Next Check Time:	2010/11/30 17:23:22
Last Update Time:	2010/11/30 16:23:22
Server Response:	MyCloudNAS name and WAN IP updated successfully.

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>).

CONFIGURE MYCLOUDNAS
PUBLISH SERVICES

Publish Services

You can publish NAS services to MyCloudNAS website (<http://www.mycloudnas.com>).

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 QCloud Access Code.

NAS Services	Enable	Publish	Private
Web Administration	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web File Manager	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web Server	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Multimedia Station	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Secure Web Administration	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure Web File Manager	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure Web Server	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure Multimedia Station	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

MyCloudNAS Access Code

Set the MyCloudNAS Access Code:

Note: The code must be 6-16 characters (a-z, A-Z, 0-9 only).

Click "Add Users" and specify maximum 9 local NAS users who are allowed to view the private NAS services published on MyCloudNAS website.

User Management

Click "Add User" and specify the local NAS users who are allowed to view the private NAS services published on MyCloudNAS website. These users may also use the MyCloudNAS Connect at the same time for remote access. Maximum 9 users can be specified.

Select the users and click "Send Invitation" to send an email with instruction to access the services.

<input type="checkbox"/>	User Name	MyCloudNAS Connect (VPN)	MyCloudNAS Website
<input checked="" type="checkbox"/>	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	User7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	User1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Select the connection method: MyCloudNAS Connect (VPN) utility and/or MyCloudNAS website. Click "Add".

Select users and their privileges X

Number of users selected: 3

Total: 14 ⏪ ⏩ 1 / 2 ⏪ ⏩

User Name	MyCloudNAS Connect (VPN)	MyCloudNAS Website
A0010	<input type="checkbox"/>	<input checked="" type="checkbox"/>
!!	<input type="checkbox"/>	<input type="checkbox"/>
avahi	<input type="checkbox"/>	<input type="checkbox"/>
messagebus	<input type="checkbox"/>	<input type="checkbox"/>
tomcat	<input type="checkbox"/>	<input type="checkbox"/>
avahi-autoipd	<input type="checkbox"/>	<input type="checkbox"/>
aaa	<input checked="" type="checkbox"/>	<input type="checkbox"/>
openldap	<input type="checkbox"/>	<input type="checkbox"/>
Akon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
KennyG	<input type="checkbox"/>	<input type="checkbox"/>

Click "Apply" to save the settings.

User Management

Click "Add User" and specify the local NAS users who are allowed to view the private NAS services published on MyCloudNAS website. These users may also use the MyCloudNAS Connect at the same time for remote access. Maximum 9 users can be specified.

Select the users and click "Send Invitation" to send an email with instruction to access the services.

[Add Users](#)

<input type="checkbox"/>	User Name	MyCloudNAS Connect (VPN)	MyCloudNAS Website
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	User7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	User1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	A0010	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Akon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	aaa	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Delete](#)[Send Invitation](#)

[APPLY](#)

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".

User Management

Click "Add User" and specify the local NAS users who are allowed to view the private NAS services published on MyCloudNAS website. These users may also use the MyCloudNAS Connect at the same time for remote access. Maximum 9 users can be specified.

Select the users and click "Send Invitation" to send an email with instruction to access the services.

<input type="checkbox"/>	User Name	MyCloudNAS Connect (VPN)	MyCloudNAS Website
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	User7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	User1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	A0010	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Akon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	aaa	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

Invite users with email notification to access service

User Name	Email	Reset Password ⓘ	Status
User7	<input type="text"/>	<input checked="" type="checkbox"/>	

SEND CLOSE

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.

Home >> MyCloudNAS Service >> Auto Router Configuration
Welcome admin | [Logout](#)
English

Auto Router Configuration

Auto Router Configuration

Enable UPnP Port Forwarding

Enable this function to allow access to your NAS from the Internet via an UPnP router.

Note: This function only works with the UPnP supported devices.



Status: Found UPnP router on the network ([view details](#))

Forwarded Services

Enabled	Status	Service Name	Ports	Protocol
<input checked="" type="checkbox"/>	OK	Web Administration (includes Web File Manager, Download Station, Surveillance Station)	8080	TCP
<input checked="" type="checkbox"/>	OK	Secure Web Administration	443	TCP
<input checked="" type="checkbox"/>	OK	FTP/FTPS with SSL/TLS Server	20,21	TCP
<input checked="" type="checkbox"/>	OK	Telnet Server	13131	TCP
<input checked="" type="checkbox"/>	OK	SSH/SFTP Server	22	TCP
<input checked="" type="checkbox"/>	OK	Web Server/Multimedia Station	80	TCP
<input checked="" type="checkbox"/>	OK	Secure Web Server	8081	TCP
<input type="checkbox"/>	--	Remote Replication	873	TCP

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.

Home >> MyCloudNAS Service >> Auto Router Configuration

Auto Router Configuration

Auto Router Configuration

Enable UPnP Port Forwarding

Enable this function to allow access to your NAS from the Internet via an UPnP router.

Note: This function only works with the UPnP supported devices.



Status: No UPnP router found on the network 

RESCAN



Your router does not support UPnP protocol or you have not enabled the UPnP function on the router.

[UPnP Router Compatibility Feedback...](#)

OK

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.

Forwarded Services

APPLY TO ROUTER

Enabled	Status	Service Name	Ports	Protocol
<input checked="" type="checkbox"/>	OK	Web Administration (includes Web File Manager, Download Station, Surveillance Station)	8080	TCP
<input checked="" type="checkbox"/>	OK	Secure Web Administration	443	TCP
<input checked="" type="checkbox"/>	OK	FTP/FTPS with SSL/TLS Server	20,21	TCP
<input checked="" type="checkbox"/>	OK	Telnet Server	13131	TCP
<input checked="" type="checkbox"/>	OK	SSH/SFTP Server	22	TCP
<input checked="" type="checkbox"/>	OK	Web Server/Multimedia Station	80	TCP
<input checked="" type="checkbox"/>	OK	Secure Web Server	8081	TCP
<input type="checkbox"/>	--	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 Information⁶⁶⁶

System Service⁶⁶⁷

Resource Monitor⁶⁶⁸

11.1 System Information

You can view the system information such as CPU usage and memory on this page.

Home >> System Status >> System Information Welcome admin | Logout English

System Information

System Information

Server Name	nas
Firmware Version	3.5.0 Build 0822T
System Up Time	0 day 8 Hour 28 Minute(s)
Serial Number	Q10AI07669

Port Status

Port No.	Port Status	IP Address	MAC Address	Packets Received	Packets Sent	Error Packets
Ethernet 1	Up	10.8.13.59	00:08:9B:C5:A3:01	2802369	3491493	0

Hardware Information

CPU Usage	13.6 %
Total Memory	503.4 MB
Free Memory	396.3 MB
System Temperature	45°C/113°F
HDD 1 Temperature	41°C/105°F

11.2 System Service

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

System Service

System Service

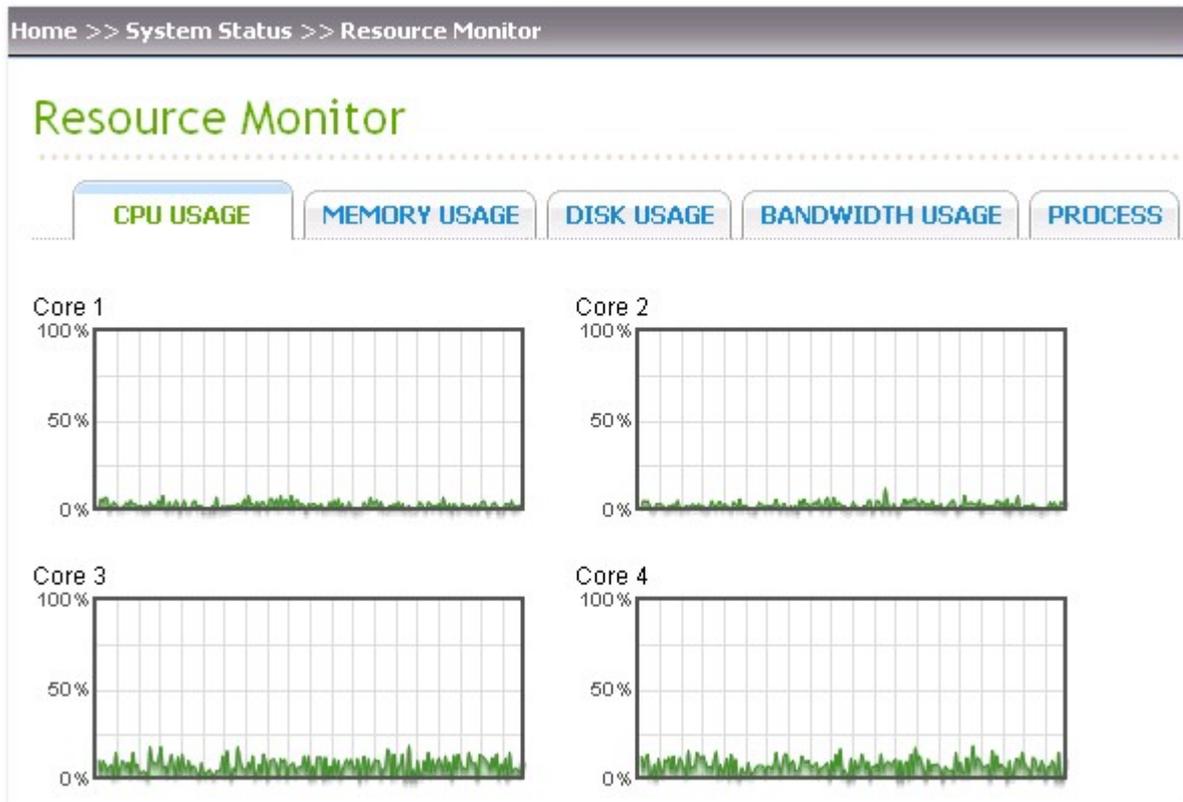
Microsoft Networking	
Enabled	<input checked="" type="checkbox"/>
Server Type	Standalone Server
Workgroup	NAS
Enable WINS server	<input type="checkbox"/>
Enable Local Master Browser	<input checked="" type="checkbox"/>
Apple Networking	
Enabled	<input type="checkbox"/>
Apple Zone Name	*
Unix/Linux NFS	
Enabled	<input type="checkbox"/>
Web File Manager	
Enabled	<input checked="" type="checkbox"/>
FTP Service	
Enabled	<input checked="" type="checkbox"/>
Port	21
Maximum Connections	30
System Port Management	
Port	8080

Multimedia Station	
Enable Multimedia Station	<input checked="" type="checkbox"/>
Enable iTunes Service	<input type="checkbox"/>
Enable UPnP Media Server	<input type="checkbox"/>
Download Station	
Enabled	<input checked="" type="checkbox"/>
Web Server	
Enabled	<input checked="" type="checkbox"/>
Port	80
register_globals	<input type="checkbox"/>
DDNS Service	
Enabled	<input type="checkbox"/>
MySQL Server	
Enabled	<input type="checkbox"/>
Enable TCP/IP Networking	<input type="checkbox"/>
Surveillance Station	
Enabled	<input type="checkbox"/>

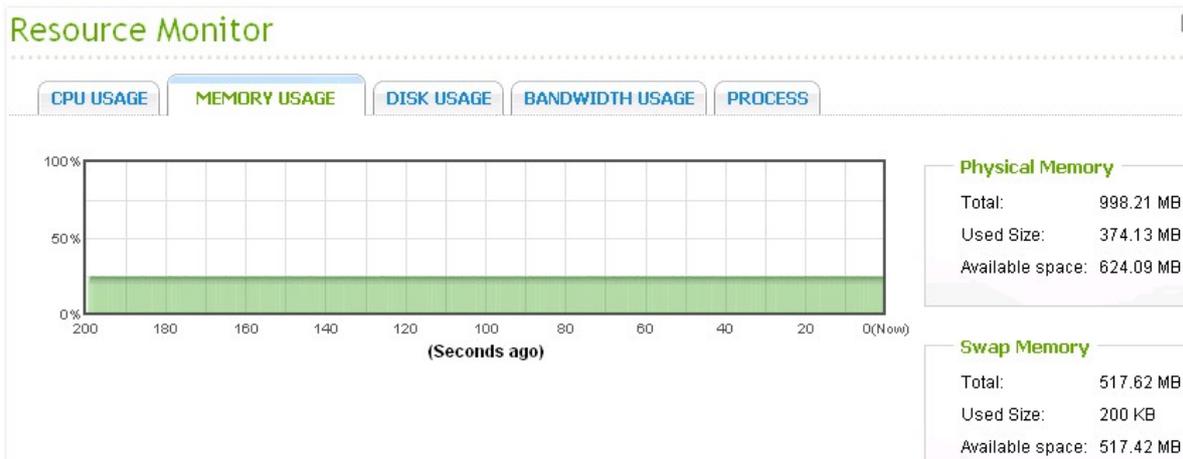
11.3 Resource Monitor

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

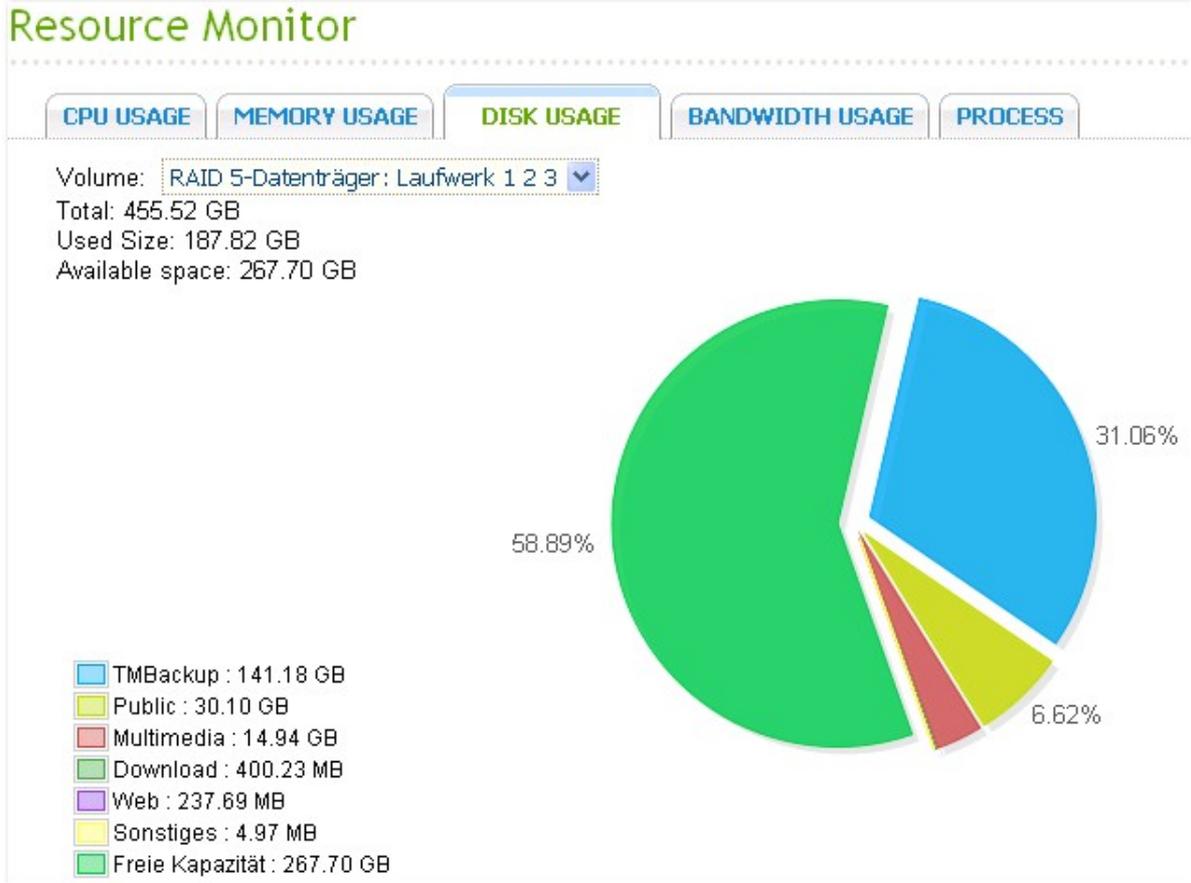
CPU Usage: This tab shows the CPU usage of the NAS.



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.

Resource Monitor

CPU USAGE MEMORY USAGE DISK USAGE BANDWIDTH USAGE **PROCESS**

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
qVvatcodogcd: 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.

C	P	U		T	e	m	p	:		5	0	°	C		
S	y	s		T	e	m	p	:		5	5	°	C		

S	y	s		F	a	n	:	8	6	5	R	P	M		

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.

C	h	a	n	g	e		P	a	s	s	w	o	r	d	
					Y	e	s		→	N	o				

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.

N	e	w		P	a	s	s	w	o	r	d	:			
														O	K

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.

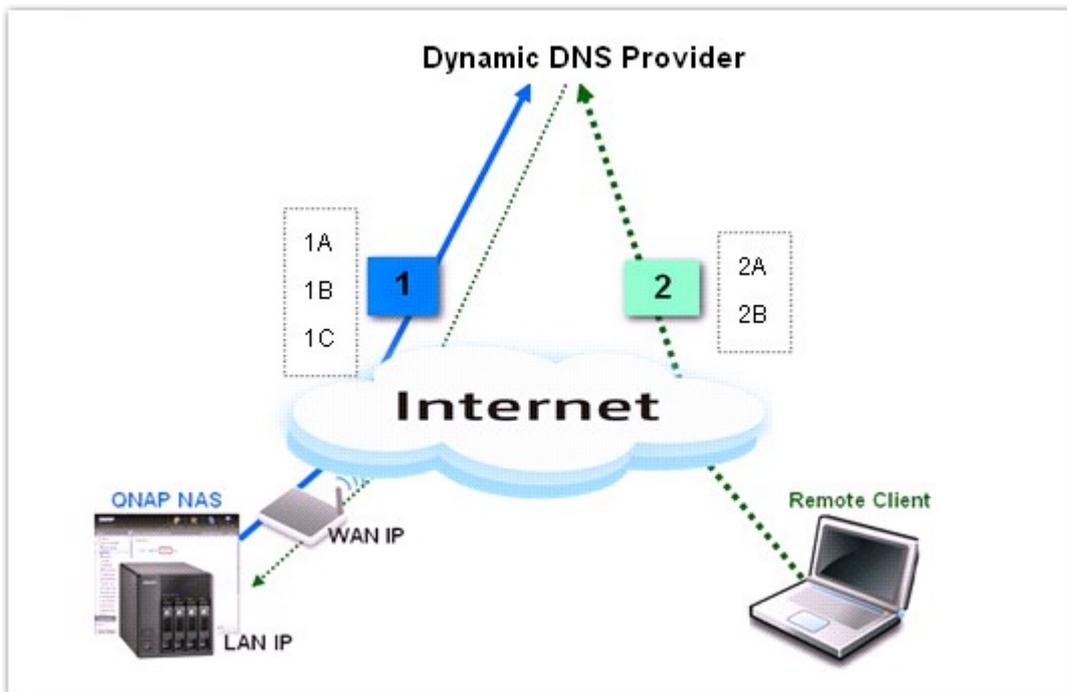
S	y	s	t	e	m		E	r	r	o	r	!			
P	l	s	.		C	h	e	c	k		L	o	g	s	

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 provider to ensure it is always available for remote access.



1A: Register a host name from a DDNS provider.

1B: Enable the DDNS service and enter the DDNS account information on the NAS.

1C: The NAS will update the WAN IP information to the DDNS provider automatically.

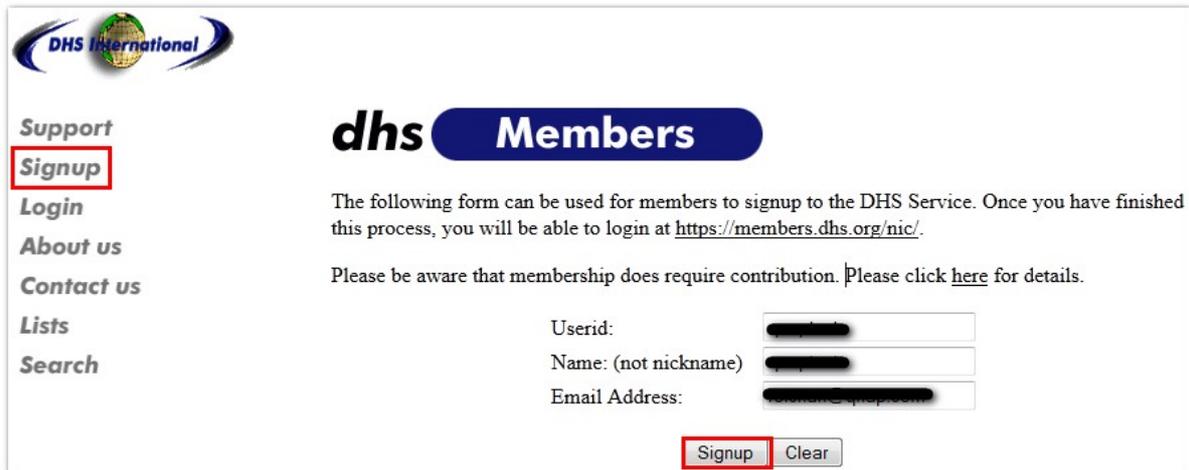
2A: Connect to the NAS by the registered host name.

2B: The DDNS provider will map the WAN IP updated by the NAS to the host 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. The Turbo 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.dhs.org as an example. Visit http://www.dhs.org. Under "Signup" create an account. Then click "Signup".





Support
Signup
Login
About us
Contact us
Lists
Search

dhs Members

The following form can be used for members to signup to the DHS Service. Once you have finished this process, you will be able to login at <https://members.dhs.org/nic/>.

Please be aware that membership does require contribution. Please click [here](#) for details.

Userid:

Name: (not nickname)

Email Address:

Signup

3. Agree to the terms of service.

dhs Members

In order to become a member you must agree to the following Terms of Service.

Agree to terms of Service

TERMS OF SERVICE

This Agreement contains all of the terms and conditions between DHS International Pty Ltd ("DHS"), and the individual or organization ("user") participating in services from "DHS".

In this Agreement, "we" and "us" means "DHS International Pty Ltd", and "you" means the "user" participating in the services. "DHS International Web Site" or "Our Site" means the web site located at <http://www.dhs.org> or any other of the sites "DHS" has under its direct control, and "Your Site" means the site(s) which you, the user, use our hostnames to resolve to. "Services" means any such services that DHS International may provide to users.

1. Registration at DHS International.

To begin the registration process, you must submit a properly completed registration application via Our Site. We will evaluate your application in good faith and will notify you of your acceptance or rejection in a timely manner. We may reject your application at any time if we determine, in our sole discretion, that Your Site is unsuitable for resolution from one of our hostnames. Your Site may be deemed by us to be unsuitable if, in our view, it:

i. contains, promotes or links to sexually explicit or violent material;

4. A confirmation email will be sent to the email address.

dhs Members

Account created.

Your account has been created and details have been emailed to [REDACTED]. Inside that email are the details on how to activate your account so you can login to the Members area.

[Back to members](#)

5. Enter the user ID and code in the email to activate the account.

dhs Members

Your two steps away from accessing all the members services. Please insert the information from the email which you recieved.

Userid:

Code:

6. Set a password for your login ID.



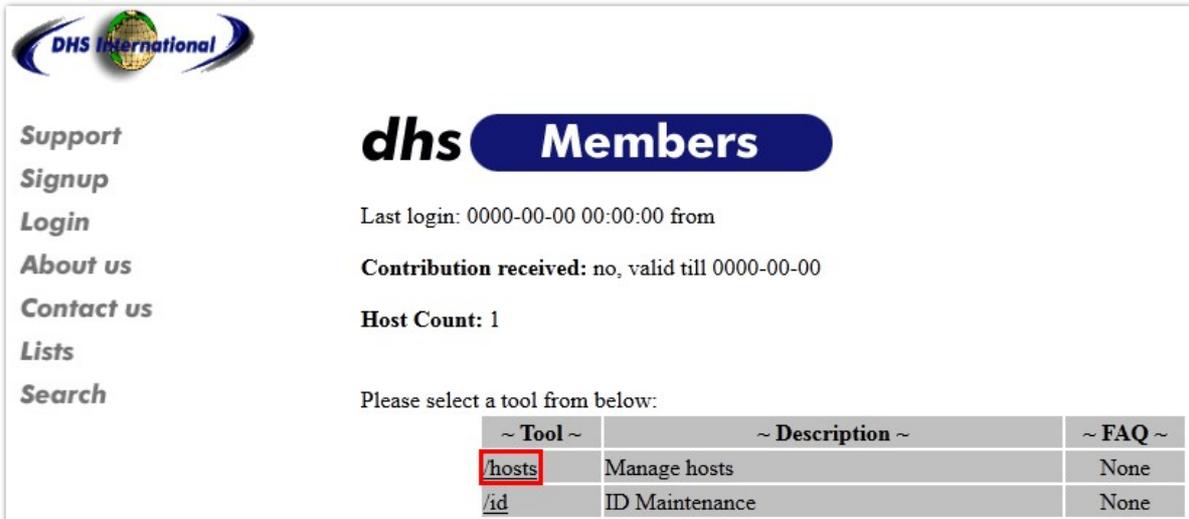
dhs **Members**

Code verified.

We now need you to set a password on your login id.

Password:

7. Login your account and click "hosts" to add a host.



DHS International

dhs Members

Support
Signup
Login
About us
Contact us
Lists
Search

Last login: 0000-00-00 00:00:00 from
Contribution received: no, valid till 0000-00-00
Host Count: 1

Please select a tool from below:

~ Tool ~	~ Description ~	~ FAQ ~
/hosts	Manage hosts	None
/id	ID Maintenance	None

8. Click "Add".

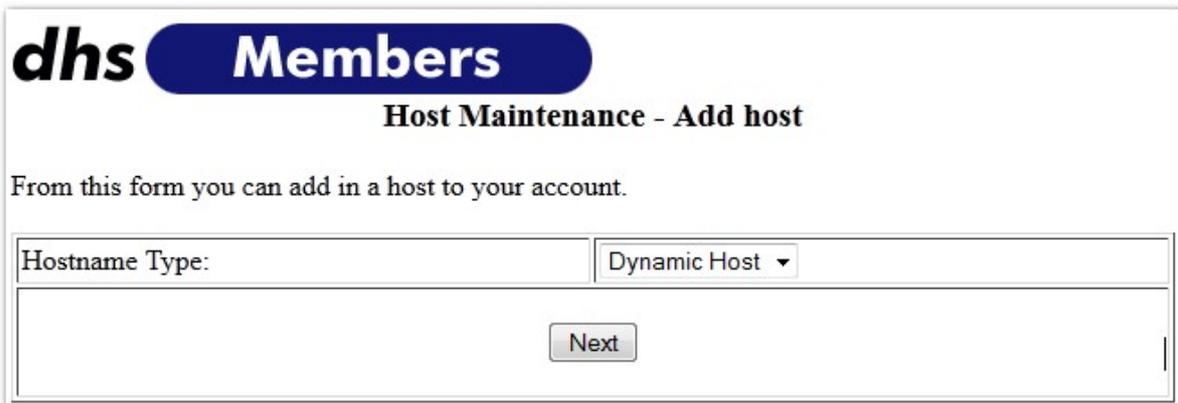


dhs Members

Host Maintenance

Add Edit Delete

9. Select a host type and click "Next".



dhs Members

Host Maintenance - Add host

From this form you can add in a host to your account.

Hostname Type: Dynamic Host ▾

Next

10. Enter the host name and the WAN IP of the NAS. Click "Add".

dhs Members

Host Maintenance - Add AtHome host

Domain:	home.dhs.org ▾
Hostname:	testestnas
Redirect to:	http:// www.testestnas.com
Cloak	<input type="checkbox"/>
Title of cloaked page:	
<input type="button" value="Add"/>	

dhs Members

Host Maintenance - Add host

Host created successfully and should be functional.

Click here to return to the [nic](#).

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.

Home >> System Administration >> Network

TCP/IP WI-FI **DDNS** IPV6

DDNS Service

After enabling DDNS Service, you can connect to this server by domain name.

Enable Dynamic DNS Service

Select DDNS server: members.dhs.org

Enter the account information you registered with the DDNS provider|

User name: [REDACTED]

Password: [REDACTED]

Host Name: [REDACTED]

Check the External IP Address Automatically 10 minutes

Current WAN IP: 59.104.86.4

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 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.

The screenshot shows the MXToolbox website interface. At the top, there is a navigation bar with links for Mx Lookup, Blacklists, Diagnostics, Analyze Headers, SPF Records, and Free Monitoring. Below the navigation bar, the page title is "SuperTool Beta7". A search input field contains the domain "testestnas.home.dhs.org" and a "Lookup" button. Below the search field, the results for "a:testestnas.home.dhs.org" are displayed, including a "Find Monitors" button and a refresh icon. A table shows the DNS record details:

Type	Domain Name	IP Address	TTL
A	testestnas.home.dhs.org	207.171.224.100	2 hrs

Below the table, there are links for "smtp diag", "blacklist", "port scan", and "http test". At the bottom, it says "Reported by ns1.dhsnames.com on Tuesday, October 30, 2012 at 3:25:41 AM (UTC -5) Transcript".

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

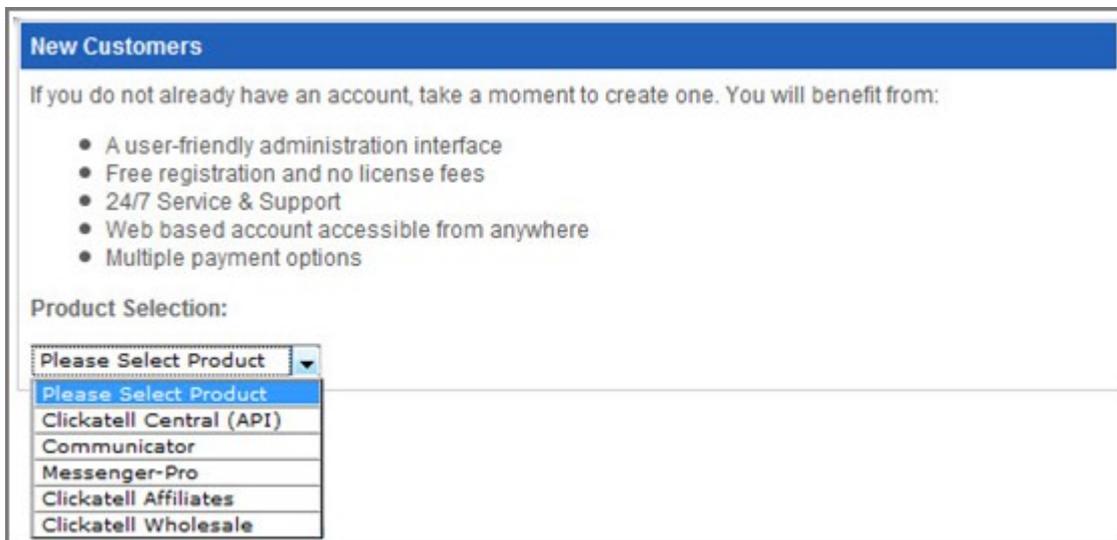
The QNAP NAS supports SMS (Short Message Service), email, and Instant Messaging (IM) alert to inform users of system error or warning.

*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)".



New Customers

If you do not already have an account, take a moment to create one. You will benefit from:

- A user-friendly administration interface
- Free registration and no license fees
- 24/7 Service & Support
- Web based account accessible from anywhere
- Multiple payment options

Product Selection:

Please Select Product ▼

- Clickatell Central (API)
- Communicator
- Messenger-Pro
- Clickatell Affiliates
- Clickatell Wholesale

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.

Complete our simple registrations process below to test our gateway and obtain your free test credits.

* Indicates all fields that are required.

Step 1 of 4 - Select Product

Select one of the products below which you would like to register for:

Clickatell Central  Communicator 

Step 2 of 4 - Account Setup

Select a country specific or international account type, based on your requirements for SMS traffic delivery destinations.

International Coverage Account:  Local Coverage Account: 

 INTERNATIONAL  USA  UK  SA

* Create Username: Security Code: 
* Create Password: *Enter Security Code:

Step 3 of 4 - Personal Information

*First Name: *Country:

* Last Name: * Mobile Number:

* Email Address:  (e.g. sample@domain.com)

Personal Use Only

* Company:

Emails sent to me must be in Text format or HTML format

I would like to receive: Clickatell News, Balance Notifications, Promotions

* I accept Clickatell's [Terms and Conditions](#)

Security & Privacy 

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".

My Account Login

Customer Login

Existing Clickatell account holders can select their product and login below. Note, username & password are CASE sensitive.

Select Product: Clickatell Central (API) ▼

Username:

ClientID:

Password:

[Lost password?](#)

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".

Verify your Mobile Number

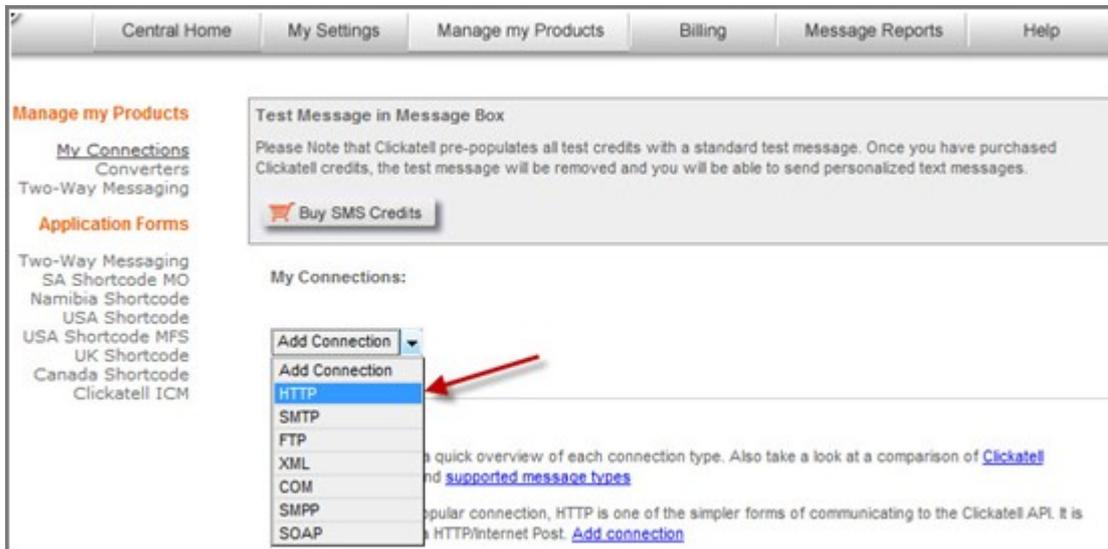
For security reasons you are required to verify your mobile number in order to make your first credit purchase and send non-test SMS messages.

Your activation code will be sent to **SEND ACTIVATION CODE**

If this is not your number, please retype your mobile number in the box above and click the "Send Activation Code" button.

Enter your activation code here: **VERIFY NOW**

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.

The screenshot shows the 'HTTP API' configuration form. The form title is 'HTTP API'. Below the title, there is a descriptive paragraph: 'This product provides an interface between your applications and the Messaging Gateway. It is a lower level connectivity option, but offers the most functionality and flexibility for the Developer and Systems Integrator. With the API you can set up alert-based SMS delivery from your server, deliver information to your mobile sales staff and keep in contact with your customers. This product is intended for machine-generated to User messaging.' Below this is a section titled 'Add HTTP API - Bold Items Required'. The form contains the following fields: 'Name:' (text input, highlighted with a red box), 'IP Lock Down:' (text input), 'Dial Prefix:' (dropdown menu, highlighted with a red box), 'Callback Type:' (dropdown menu, set to 'HTTP GET', highlighted with a red box), 'Callback Url:' (text input), 'Callback Username:' (text input), and 'Callback Password:' (text input). At the bottom of the form is a 'Submit' button. A note at the bottom of the form reads: 'NOTE: submission of this form will delete any session_id currently valid for this api_id. Any application using this session_id will have to re-authenticate.'

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.

<u>Name</u>	<u>Type</u>	<u>API ID</u> ▾	<u>Dialing Code</u>
██████████	HTTP	██████████	886 Taiwan

1 to 1 of 1

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.

The screenshot shows a web application interface for configuring the SMSC server. At the top, there is a breadcrumb trail: "Home >> System Administration >> Notification". On the right, it says "Welcome admin | Logout" and "English". Below the breadcrumb is the "Notification" section with four tabs: "CONFIGURE SMTP SERVER", "CONFIGURE IM", "CONFIGURE SMSC SERVER" (which is active), and "ALERT NOTIFICATION".

The "Configure SMSC Server" section contains the following fields and options:

- A description: "You can configure the SMSC settings to send instant system alerts via the SMS service provided by the SMS provider."
- "SMS Service Provider": A dropdown menu with "Clickatell" selected and a URL "http://www.clickatell.com" displayed next to it.
- "Enable SSL Connection": A checked checkbox.
- "SSL Port": A text input field containing "443".
- "SMS Server Login Name": A text input field with a blurred value.
- "SMS Server Login Password": A password input field with masked characters (dots).
- "SMS Server API_ID": A text input field with a blurred value.

An "APPLY" button is located at the bottom right of the form.

Next go to "System Administration" > "Notification" > "Alert Notification" and enter the mobile number (max 2) to receive the alert.

Home >> System Administration >> Notification Welcome admin | Logout

[CONFIGURE SMTP SERVER](#) [CONFIGURE IM](#) [CONFIGURE SMSC SERVER](#) **ALERT NOTIFICATION**

Alert Notification

When a system event occurs, do the following immediately:

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](#)

SMS Notification Settings

Country Code:

Cell Phone No. 1: +886

Cell Phone No. 2: +886

[SEND A TEST SMS MESSAGE](#)

Note: You must configure the SMSC server to be able to send SMS notification properly.

Congratulations! It is all set up and now you may want to test if you have configured 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.

The screenshot shows the 'Notification' section of a web interface. The breadcrumb trail is 'Home >> System Administration >> Notification'. The user is logged in as 'admin' and the language is set to 'English'. There are four tabs: 'CONFIGURE SMTP SERVER' (active), 'CONFIGURE IM', 'CONFIGURE SMSC SERVER', and 'ALERT NOTIFICATION'. The 'Configure SMTP Server' section contains the following fields and options:

- SMTP Server:
- Port Number:
- Sender:
- Enable SMTP Authentication
 - User Name:
 - Password:
- Use SSL/TLS secure connection
 - Protocol Type:

An 'APPLY' button is located at the bottom right of the configuration area.

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".

The screenshot shows the 'Alert Notification' section of the web interface. The breadcrumb trail is 'Home >> System Administration >> Notification'. The user is logged in as 'admin' and the language is set to 'English'. There are four tabs: 'CONFIGURE SMTP SERVER', 'CONFIGURE IM', 'CONFIGURE SMSC SERVER', and 'ALERT NOTIFICATION' (active). The 'Alert Notification' section contains the following options:

When a system event occurs, do the following immediately:

- Send system error alert by: Email SMS Instant Messaging
- Send system warning alert by: Email Instant Messaging

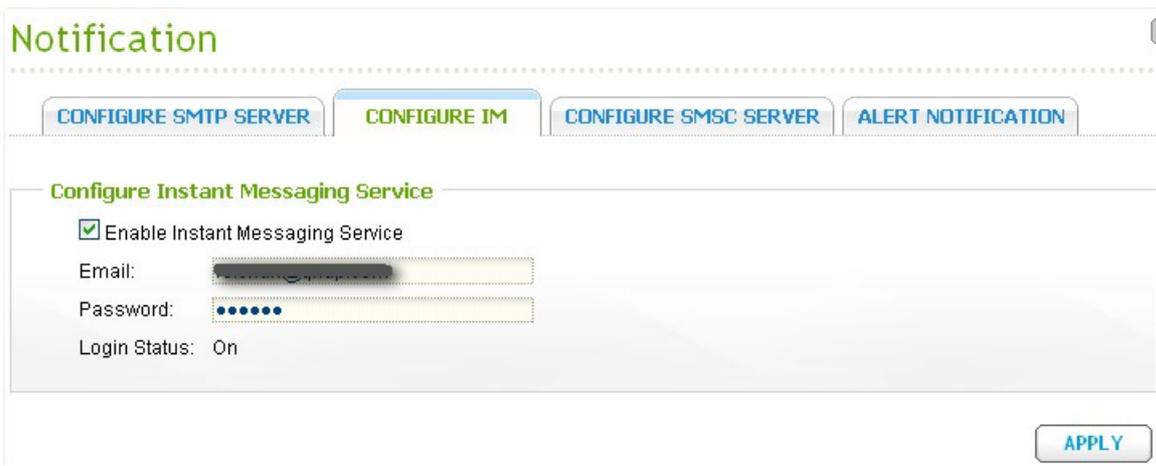
The 'E-mail Notification Settings' section contains the following fields and options:

- E-mail address 1:
- E-mail address 2:
-

A note at the bottom states: "Note: The SMTP server must be configured first for alert mail delivery."

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".



The screenshot shows a web-based configuration interface titled "Notification". At the top, there are four tabs: "CONFIGURE SMTP SERVER", "CONFIGURE IM" (which is selected and highlighted in green), "CONFIGURE SMSC SERVER", and "ALERT NOTIFICATION". Below the tabs, the "Configure Instant Messaging Service" section is visible. It contains a checked checkbox labeled "Enable Instant Messaging Service". Below this, there are two input fields: "Email:" with a masked value and "Password:" with five dots. At the bottom left of this section, the "Login Status:" is displayed as "On". An "APPLY" button is located at the bottom right of the configuration area.

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".

The screenshot shows a web interface for configuring notifications. At the top, there are four tabs: "CONFIGURE SMTP SERVER", "CONFIGURE IM", "CONFIGURE SMSC SERVER", and "ALERT NOTIFICATION". The "ALERT NOTIFICATION" tab is selected and highlighted in green. Below the tabs, the "Alert Notification" section is titled in green. It contains a red-bordered box with the following text: "When a system event occurs, an alert email/SMS will be sent automatically." Below this, there are two lines of configuration: "Send system error alert by:" with radio buttons for "Email", "SMS", and "Instant Messaging" (which is checked); and "Send system warning alert by:" with radio buttons for "Email" and "Instant Messaging" (which is checked). Below this section is the "E-mail Notification Settings" section, which has two input fields for "E-mail address 1:" and "E-mail address 2:", and a "SEND A TEST E-MAIL" button. A note below reads: "Note: The SMTP server must be configured first for alert mail delivery." At the bottom is the "Instant Messaging Settings" section, also highlighted with a red border. It features an "Authorized Contacts:" label, an input field, and an "Add" button. Below the input field, there are two rows, each with a blurred input field and a "Remove" button.

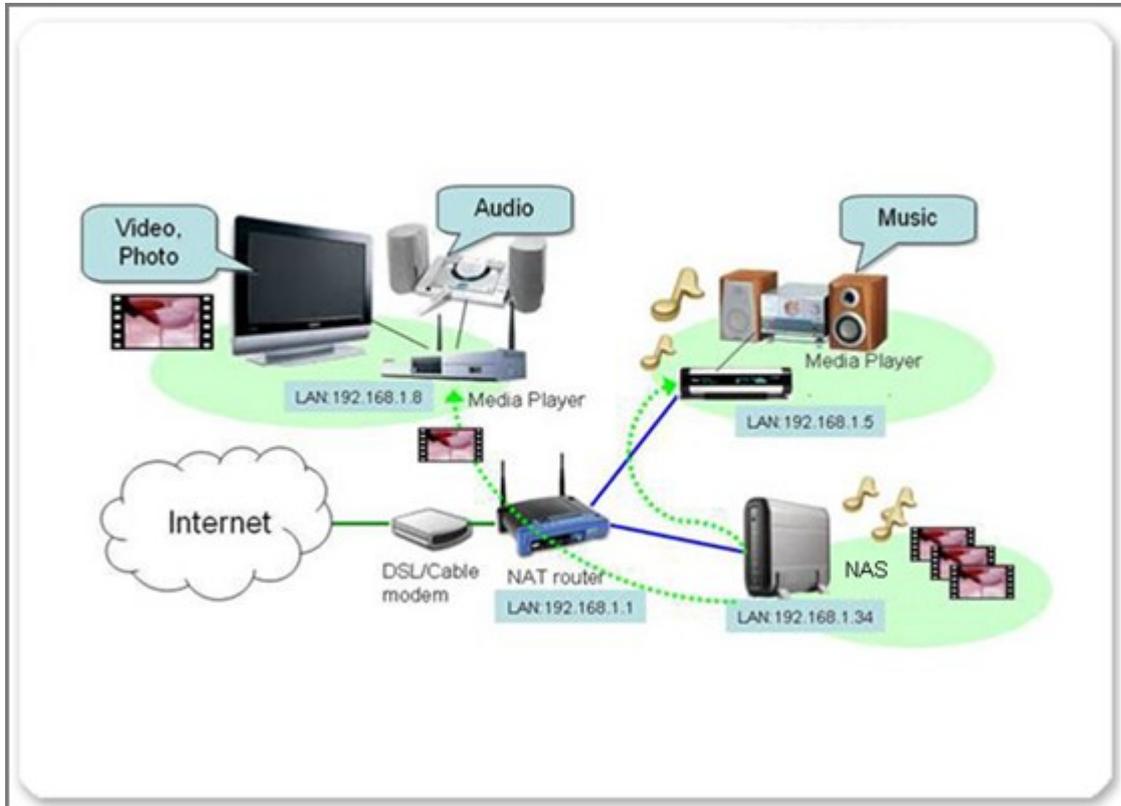
6. Login an authorized Windows Live Messenger account and interact with the NAS via Windows Live Messenger. The NAS will send instant error or warning alerts (English only) to the authorized contacts when events occur.

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 DLNA media server on QNAP NAS to share the multimedia files to the media players on the local network and play them in the home entertainment system.



Enable DLNA Media Server

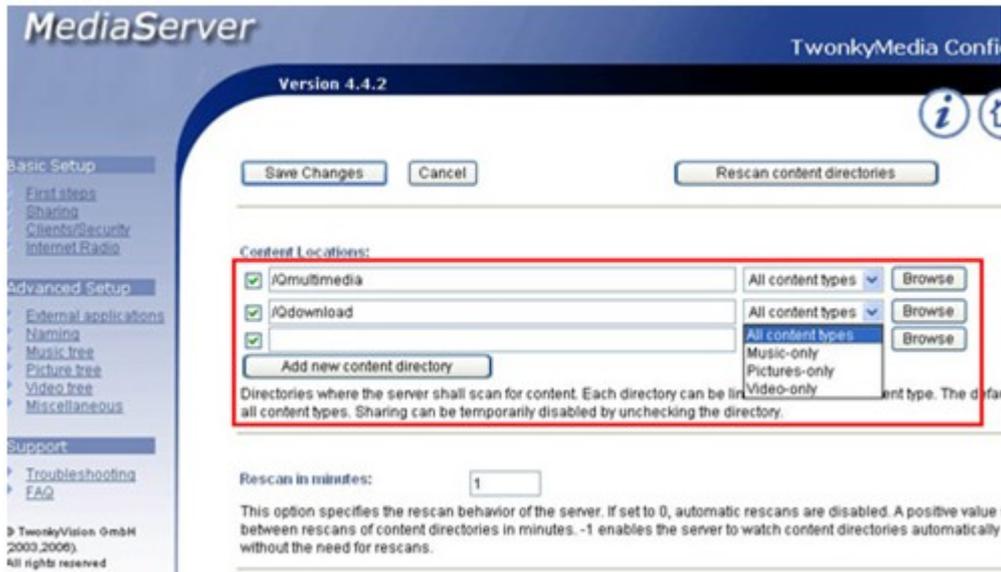
Go to "Applications" > "DLNA Media Server" and select the option "Enabled DLNA Media Server" and click "Apply". The media server function is now ready.



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 as 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.

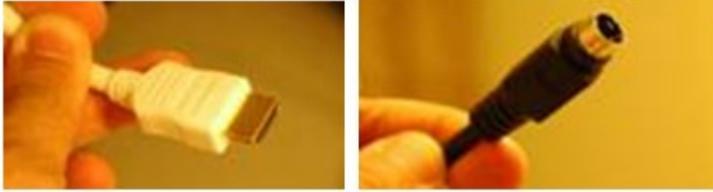


About TCP/IP settings

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)

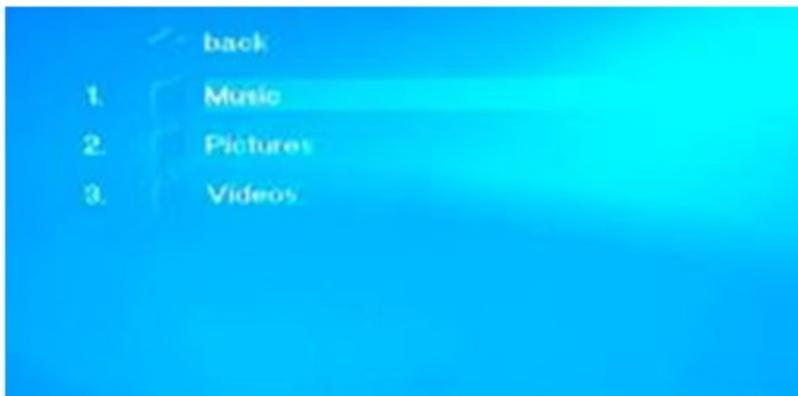
In this example, the video out and audio out cables are connected to the TV. You can also connect audio out to your stereo acoustic system.



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.

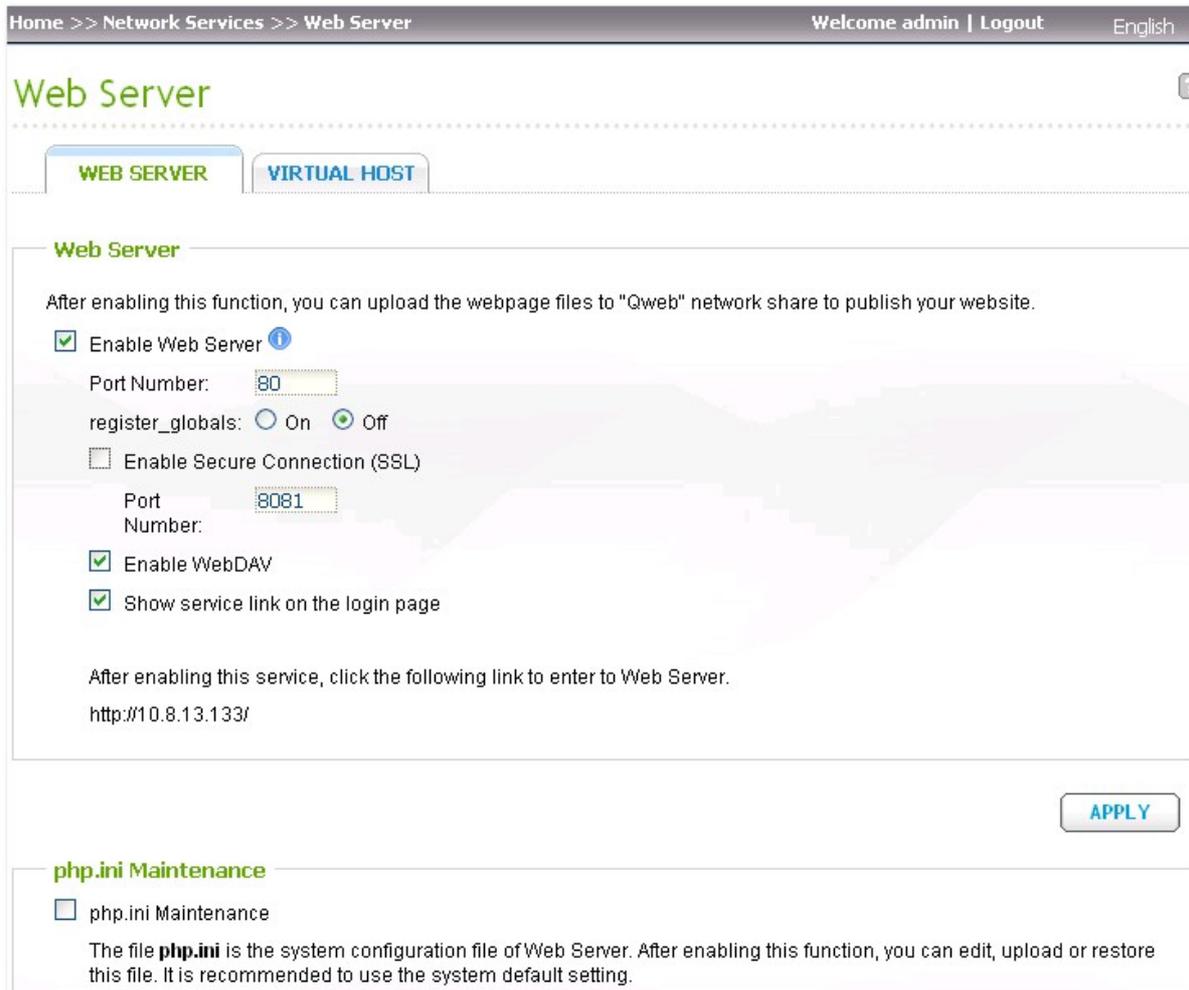


16. Host a Forum with phpBB on QNAP NAS

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".



The screenshot shows the QNAP NAS administration interface. At the top, there is a navigation bar with "Home >> Network Services >> Web Server", a user greeting "Welcome admin | Logout", and a language selector "English". Below the navigation bar, the page title "Web Server" is displayed in green. There are two tabs: "WEB SERVER" (active) and "VIRTUAL HOST".

The main content area is titled "Web Server" and contains the following text: "After enabling this function, you can upload the webpage files to 'Qweb' network share to publish your website." Below this text are several configuration options:

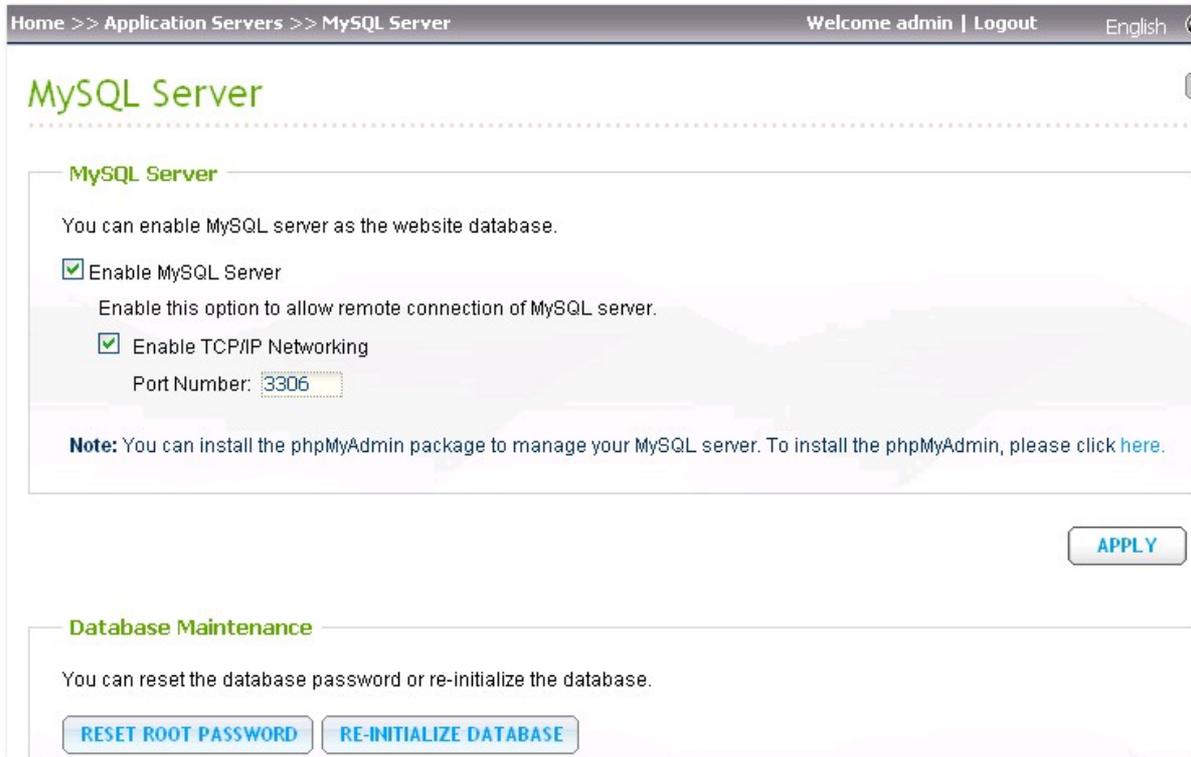
- Enable Web Server ⓘ
- Port Number:
- register_globals: On Off
- Enable Secure Connection (SSL)
- Port Number:
- Enable WebDAV
- Show service link on the login page

Below these options, there is a note: "After enabling this service, click the following link to enter to Web Server." followed by the URL "http://10.8.13.133/".

At the bottom right of the configuration area, there is a blue "APPLY" button.

The bottom section of the page is titled "php.ini Maintenance" and contains the following text: "The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting." Below this text is a checkbox labeled "php.ini Maintenance" which is currently unchecked.

Next go to "Applications" > "MySQL Server" and select both "Enable MySQL Server" and "Enable TCP/IP Networking" then click "Apply".



The screenshot shows a web interface for configuring the MySQL Server. At the top, there is a breadcrumb trail: "Home >> Application Servers >> MySQL Server". On the right side of the header, it says "Welcome admin | Logout" and "English". The main heading is "MySQL Server".

Under the heading, there is a section titled "MySQL Server". Below this title, it says "You can enable MySQL server as the website database." There are two checked checkboxes: "Enable MySQL Server" and "Enable TCP/IP Networking". Below the second checkbox, there is a text input field for "Port Number" with the value "3306".

A note below the checkboxes reads: "Note: You can install the phpMyAdmin package to manage your MySQL server. To install the phpMyAdmin, please click [here](#)." To the right of this section is an "APPLY" button.

Below the "MySQL Server" section is a section titled "Database Maintenance". It says "You can reset the database password or re-initialize the database." At the bottom of this section are two buttons: "RESET ROOT PASSWORD" and "RE-INITIALIZE DATABASE".

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 username and password to login (default username 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

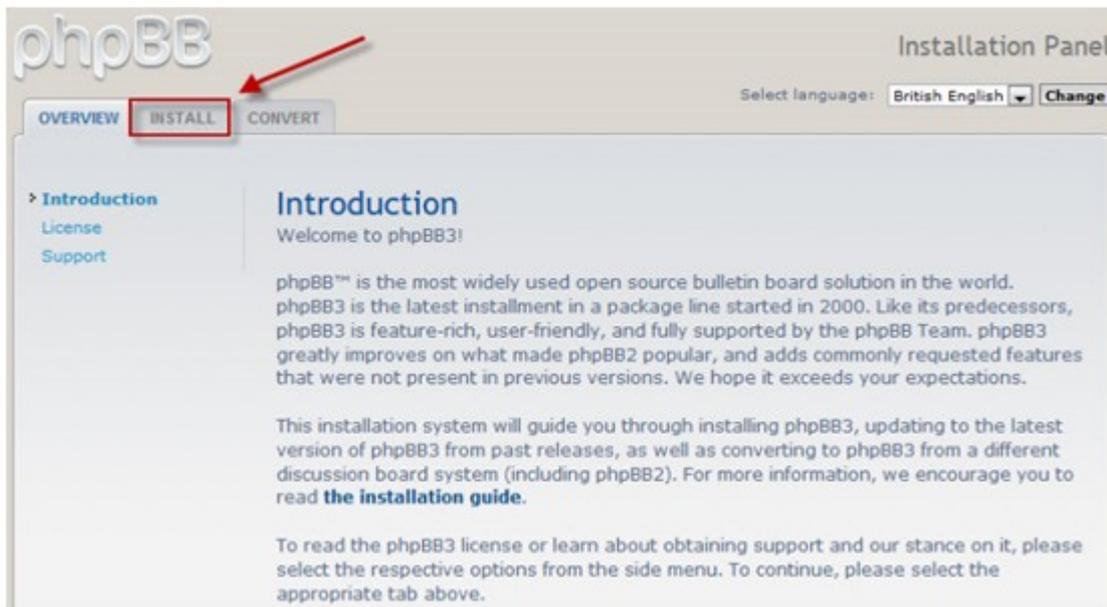
Download the phpbb3 source archive from <http://www.phpbb.com/downloads/olympus.php> and download the [Full Package] one and unzip it to Qweb or Web network share.

[Full Package]
Contains entire phpBB3 source and english language files.
Best suited for new installations.

 [Download phpBB 3.0.5 \(zip\)](#)
Size: 2.22 MiB
md5sum: 69c4ec3f1495e518c6b8a5dac8543ab4

 [Download phpBB 3.0.5 \(bz2\)](#)
Size: 1.43 MiB
md5sum: 734b8f9c2390d5cc8c971cfc29da185

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.



The screenshot shows the phpBB3 Installation Panel. At the top left is the phpBB logo. On the right, it says "Installation Panel" and "Select language: British English" with a "Change" button. Below the logo are three tabs: "OVERVIEW", "INSTALL" (highlighted with a red box and a red arrow), and "CONVERT". The main content area has a left sidebar with "Introduction", "License", and "Support" links. The main content area has a heading "Introduction" and the text: "Welcome to phpBB3! phpBB™ is the most widely used open source bulletin board solution in the world. phpBB3 is the latest installment in a package line started in 2000. Like its predecessors, phpBB3 is feature-rich, user-friendly, and fully supported by the phpBB Team. phpBB3 greatly improves on what made phpBB2 popular, and adds commonly requested features that were not present in previous versions. We hope it exceeds your expectations. This installation system will guide you through installing phpBB3, updating to the latest version of phpBB3 from past releases, as well as converting to phpBB3 from a different discussion board system (including phpBB2). For more information, we encourage you to read **the installation guide**. To read the phpBB3 license or learn about obtaining support and our stance on it, please select the respective options from the side menu. To continue, please select the appropriate tab above."

Click "Proceed to next step".

phpBB Installation Panel

Select language: British English Change

OVERVIEW **INSTALL** CONVERT

Introduction

- Requirements
- Database settings
- Administrator details
- Configuration file
- Advanced settings
- Create database tables
- Final stage

Welcome to Installation

With this option, it is possible to install phpBB3 onto your server.

In order to proceed, you will need your database settings. If you do not know your database settings, please contact your host and ask for them. You will not be able to continue without them. You need:

- The Database Type - the database you will be using.
- The Database server hostname or DSN - the address of the database server.
- The Database server port - the port of the database server (most of the time this is not needed).
- The Database name - the name of the database on the server.
- The Database username and Database password - the login data to access the database.

Note: if you are installing using SQLite, you should enter the full path to your database file in the DSN field and leave the username and password fields blank. For security reasons, you should make sure that the database file is not stored in a location accessible from the web.

phpBB3 supports the following databases:

- MySQL 3.23 or above (MySQLi supported)
- PostgreSQL 7.3+
- SQLite 2.8.2+
- Firebird 2.0+
- MS SQL Server 2000 or above (directly or via ODBC)
- Oracle

Only those databases supported on your server will be displayed.

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.

The screenshot shows the phpBB Installation Panel with the 'INSTALL' tab selected. The 'Database configuration' section is active, and a red box highlights the input fields. The fields are: Database type (MySQL), Database server hostname or DSN (127.0.0.1), Database server port (empty), Database name (phpbb3), Database username (root), Database password (masked with dots), and Prefix for tables in database (phpbb_). A 'Proceed to next step' button is highlighted with a red box and an arrow pointing to it.

phpBB Installation Panel

OVERVIEW **INSTALL** CONVERT

- Introduction
- Requirements
- Database settings**
- Administrator details
- Configuration file
- Advanced settings
- Create database tables
- Final stage

Database configuration

Database type: MySQL

Database server hostname or DSN: 127.0.0.1
DSN stands for Data Source Name and is relevant only for ODBC installs.

Database server port:
Leave this blank unless you know the server operates on a non-standard port.

Database name: phpbb3

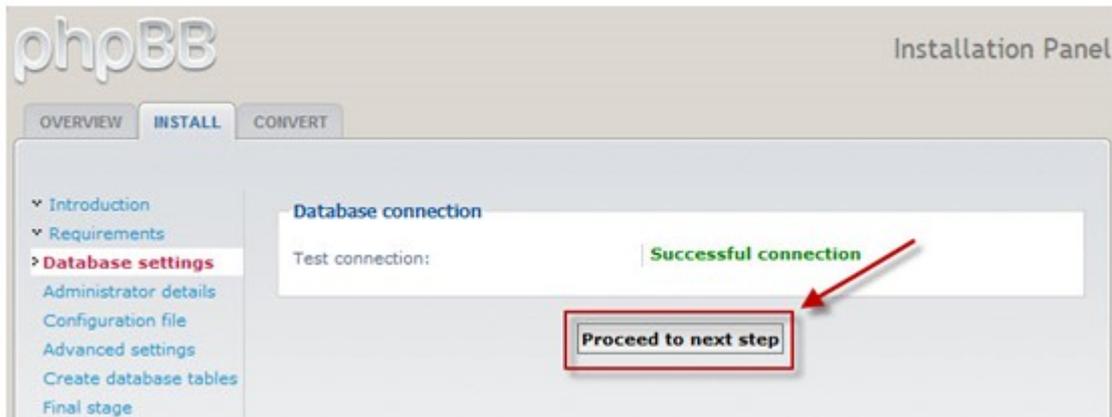
Database username: root

Database password:

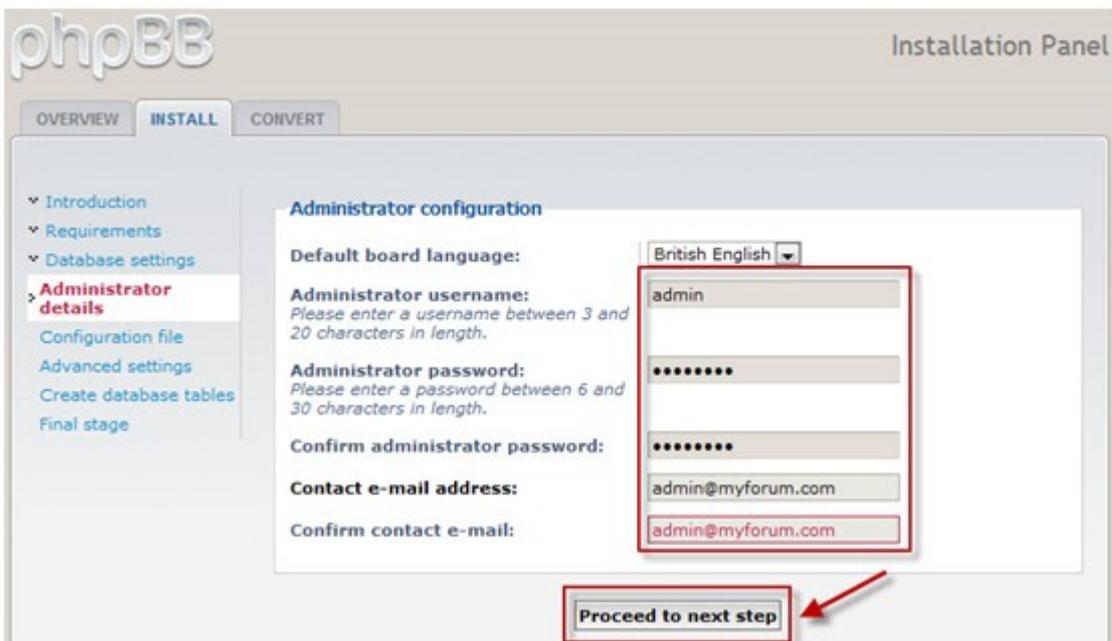
Prefix for tables in database: phpbb_

Proceed to next step

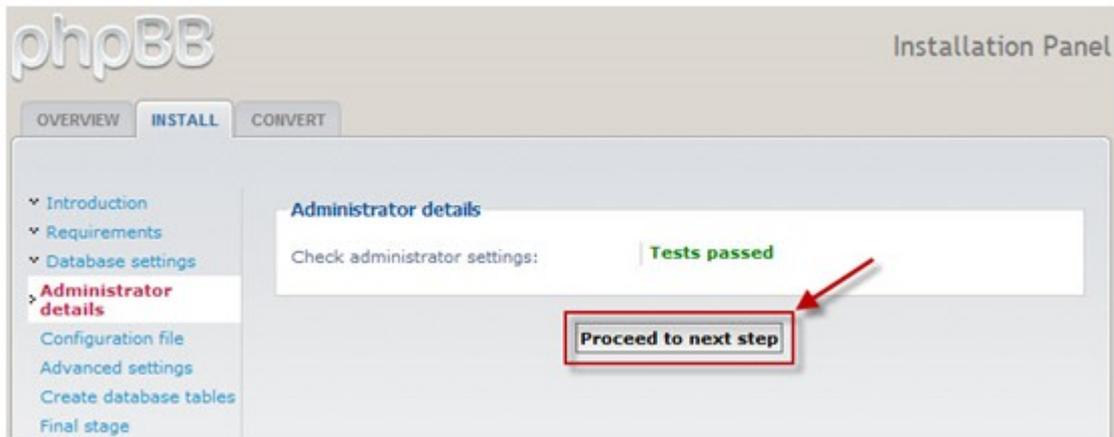
You should see "Successful connection" if your MySQL server is running and the database "phpbb3" we created earlier is present. Click "Proceed to next step".



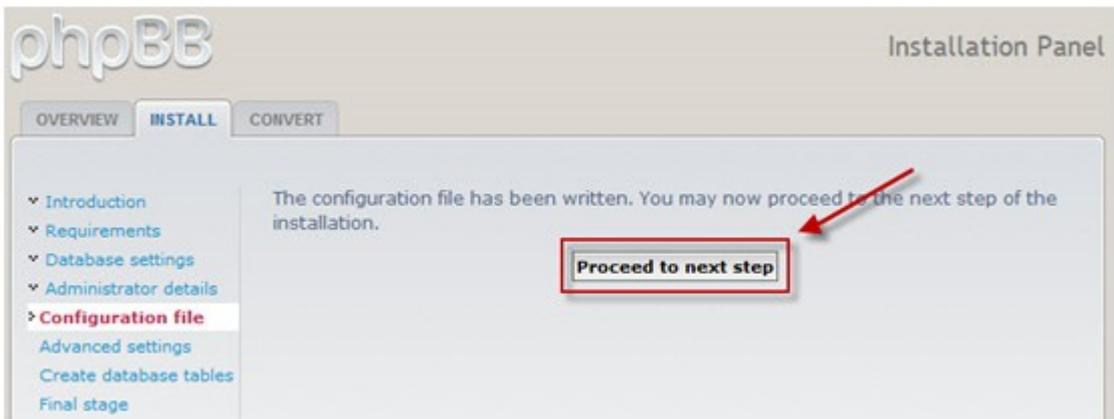
Specify the phpBB3 administrator username and password as well as a valid email address. Once done, click "Proceed to next step".



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".

The screenshot shows the 'phpBB Installation Panel' with tabs for 'OVERVIEW', 'INSTALL', and 'CONVERT'. The 'INSTALL' tab is active. On the left, a navigation menu lists: Introduction, Requirements, Database settings, Administrator details, Configuration file, **Advanced settings** (highlighted), Create database tables, and Final stage. The main content area contains the following sections:

E-mail settings

The settings on this page are only necessary to set if you know that you require something different from the default. If you are unsure, just proceed to the next page, as these settings can be altered from the Administration Control Panel later.

Enable board-wide e-mails: Enabled Disabled
If this is set to disabled no e-mails will be sent by the board at all.

Use SMTP server for e-mail: Yes No
Select "Yes" if you want or have to send e-mail via a named server instead of the local mail function.

SMTP server address:

Authentication method for SMTP: PLAIN
Only used if a username/password is set, ask your provider if you are unsure which method to use.

SMTP username:
Only enter a username if your SMTP server requires it.

SMTP password:
Only enter a password if your SMTP server requires it.

Server URL settings

Cookie secure: Enabled Disabled
If your server is running via SSL set this to enabled else leave as disabled. Having this enabled and not running via SSL will result in server errors during redirects.

Force server URL settings: Yes No
If set to yes the server settings defined here will be used in favour of the automatically determined values.

Server protocol: http://
This is used as the server protocol if these settings are forced. If empty or not forced the protocol is determined by the cookie secure settings (http:// or https://).

Domain name: 192.168.1.3
The domain name this board runs from (for example: www.example.com).

Server port: 80
The port your server is running on, usually 80, only change if different.

Script path: /phpBB3
The path where phpBB is located relative to the domain name, e.g. /phpBB3.

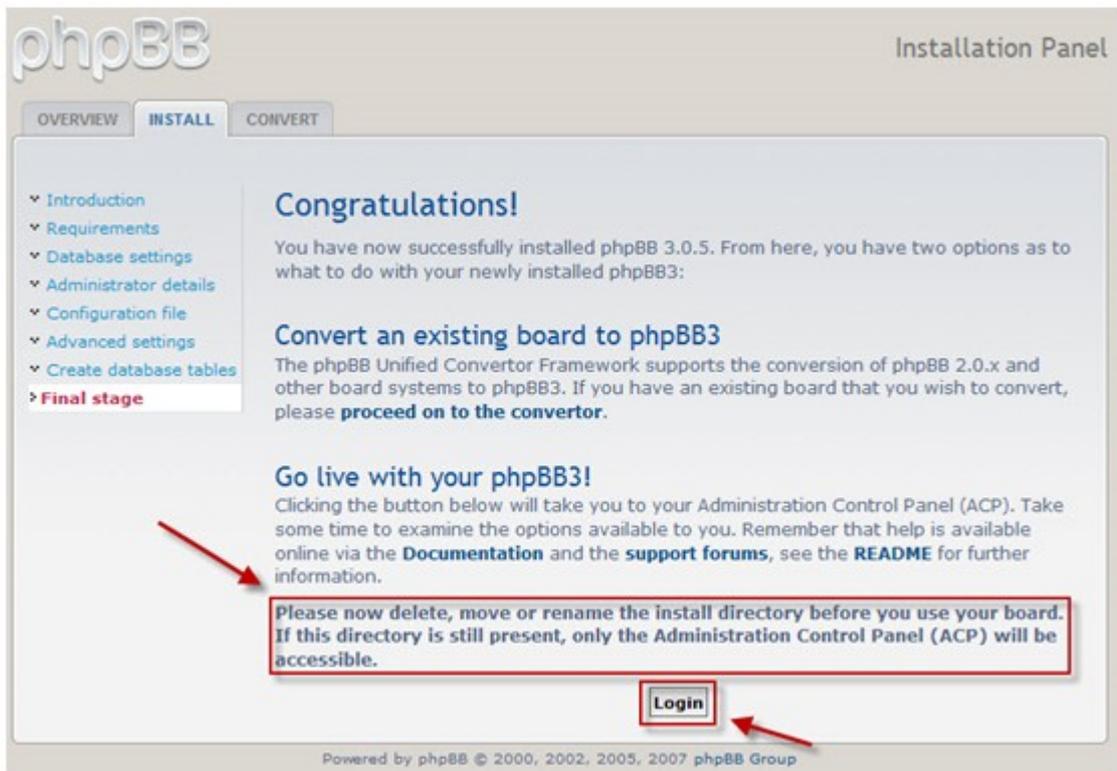
A red arrow points to a button labeled "Proceed to next step" at the bottom of the form.

Powered by phpBB © 2000, 2002, 2005, 2007 phpBB Group

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.

phpBB Administration Control Panel
Admin index + Board index

GENERAL FORUMS POSTING USERS AND GROUPS PERMISSIONS STYLES MAINTENANCE SYSTEM

You are logged in as: **admin** [Logout]
[ACP Logout]

WELCOME TO phpBB
Thank you for choosing phpBB as your board solution. This screen will give you a quick overview of all the various statistics of your board. The links on the left hand side of this screen allow you to control every aspect of your board experience. Each page will have instructions on how to use the tools.

QUICK ACCESS
Manage users
Manage groups
Manage forums
Moderator log
Spiders/Robots
PHP information

BOARD CONFIGURATION
Attachment settings
Board settings
Board features
Avatar settings
Private message settings
Post settings
Signature settings
User registration settings
Visual confirmation settings

CLIENT COMMUNICATION
Authentication
E-mail settings
Jabber settings

SERVER CONFIGURATION
Cookie settings
Server settings
Security settings
Load settings
Search settings

Board statistics

STATISTIC	VALUE	STATISTIC	VALUE
Number of posts:	1	Posts per day:	1
Number of topics:	1	Topics per day:	1
Number of users:	1	Users per day:	1
Number of attachments:	0	Attachments per day:	0.00
Board started:	Tue Jun 30, 2009 4:14 pm	Avatar directory size:	0 Bytes
Database size:	262.62 KIB	Size of posted attachments:	0 Bytes
Database server:	MySQL 5.0.67-log	GZip compression:	Off
Board version:	3.0.5	Orphan attachments:	0

Resynchronise or reset statistics

Reset most users ever online

Reset board's start date

Resynchronise statistics
Recalculates the total number of posts, topics, users and files.

Resynchronise post counts
Only existing posts will be taken into consideration. Pruned posts will not be counted.

Resynchronise dotted topics
First unmarks all topics and then correctly marks topics that have seen any activity during the past six months.

Purge the cache
Purge all cache related items, this includes any cached template files or queues.

Logged administrator actions
This gives an overview of the last five actions carried out by board administrators. A full copy of the log can be viewed from the appropriate menu item or following the link below.

[View administrator log](#)

USERNAME	USER IP	TIME	ACTION
admin	192.168.1.2	Tue Jun 30, 2009 4:14 pm	Installed phpBB 3.0.5

Inactive users
This is a list of the last 10 registered users who have inactive accounts. A full list is available from the appropriate menu item or by following the link below from where you can activate, delete or remind (by sending an e-mail) these users if you wish.

This is the front page of your freshly installed phpBB3 forum. Start sending out forum invitations to establish your online community.

phpBB yourdomain.com
creating communities A short text to describe your forum

Search... Search
Advanced search

[Board index](#) v A ^

[User Control Panel](#) (0 new messages) • [View your posts](#) [FAQ](#) [Members](#) [Logout \[admin \]](#)

It is currently Tue Jun 30, 2009 4:17 pm Last visit was: Tue Jun 30, 2009 4:14 pm
[[Moderator Control Panel](#)]

[View unanswered posts](#) • [View new posts](#) • [View active topics](#) [Mark forums read](#)

YOUR FIRST CATEGORY	TOPICS	POSTS	LAST POST
Your first forum Description of your first forum.	1	1	by admin Tue Jun 30, 2009 4:14 pm

WHO IS ONLINE

In total there are **2** users online :: 1 registered, 0 hidden and 1 guest (based on users active over the past 5 minutes)
Most users ever online was **2** on Tue Jun 30, 2009 4:17 pm

Registered users: **admin**
Legend: *Administrators*, *Global moderators*

STATISTICS

Total posts **1** • Total topics **1** • Total members **1** • Our newest member **admin**

[Board index](#) [The team](#) • [Delete all board cookies](#) • All times are UTC

Powered by phpBB © 2000, 2002, 2005, 2007 phpBB Group
[Administration Control Panel](#)

17. NAS Maintenance Settings

System Restart/Shutdown [722](#)

System Temperature Protection [725](#)

17.1 System Restart/Shutdown

By the power button

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 will beep once and shut down immediately.

*To turn off the 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.

By the web administration interface

Login the NAS as "admin". Click the triangle icon next to the login name on the top right hand corner and select to restart or shut down the NAS.



You may also restart or power off the NAS in "System Administration" > "Power Management".

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

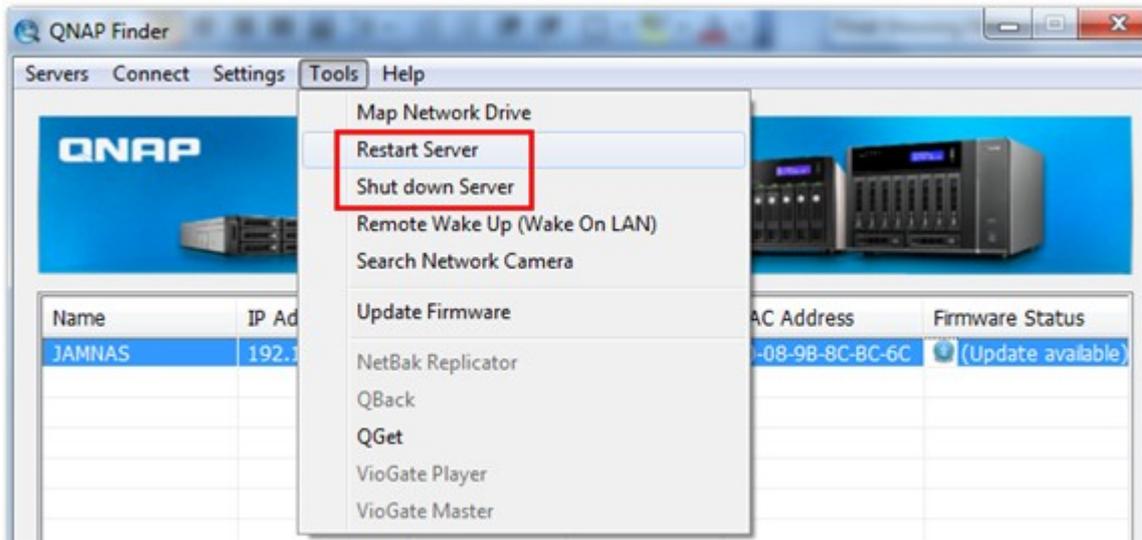
Postpone the restart/shutdown schedule when a replication job is in progress.

Shutdown Daily 7 0 +

APPLY

By the Finder

Run the Finder. Select a NAS name. Click "Tools" and select to restart or power off 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