



Turbo NAS

User Manual (Version: 3.2.0)

©2009–2010 QNAP Systems, Inc.

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

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

Legal Notices

©Copyright 2009–2010. QNAP Systems, Inc. All Rights Reserved.

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

Back up your 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.

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.

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.

Table of Contents

TABLE OF CONTENTS	5
SAFETY INFORMATION AND PRECAUTIONS.....	9
CHAPTER 1 INSTALL THE NAS.....	10
1.1 HARD DISK DRIVE COMPATIBILITY LIST	10
1.2 CHECK SYSTEM STATUS	11
CHAPTER 2 CONNECT TO THE NAS	14
CHAPTER 3 SERVER ADMINISTRATION	19
3.1 SYSTEM ADMINISTRATION.....	21
3.1.1 General Settings	22
3.1.1.1 System Administration.....	22
3.1.1.2 Date and Time	23
3.1.1.3 Daylight Saving Time	24
3.1.1.4 Language.....	25
3.1.1.5 Password Strength.....	25
3.1.2 Network.....	26
3.1.2.1 TCP/IP	26
3.1.2.2 DDNS.....	34
3.1.2.3 IPv6.....	35
3.1.3 Hardware.....	37
3.1.4 Security.....	39
3.1.4.1 Security Level.....	39
3.1.4.2 Network Access Protection.....	40
3.1.4.3 Import SSL Secure Certificate	41
3.1.5 Notification	42
3.1.5.1 Configure SMTP Server	42
3.1.5.2 Configure SMSC Server	43
3.1.5.3 Alert Notification.....	44
3.1.6 Power Management.....	45
3.1.7 Network Recycle Bin.....	47
3.1.8 Back up/ Restore Settings	48
3.1.9 System Logs	49
3.1.9.1 System Event Logs.....	49
3.1.9.2 System Connection Logs.....	50

3.1.9.3	<i>On-line Users</i>	51
3.1.9.4	<i>Syslog</i>	51
3.1.10	<i>Firmware Update</i>	52
3.1.11	<i>Restore to Factory Default</i>	55
3.2	DISK MANAGEMENT	56
3.2.1	<i>Volume Management</i>	56
3.2.2	<i>RAID Management</i>	60
3.2.3	<i>HDD SMART</i>	65
3.2.4	<i>Encrypted File System</i>	66
3.2.5	<i>iSCSI</i>	67
3.2.5.1	<i>iSCSI Target</i>	67
3.2.5.2	<i>ADVANCED ACL</i>	97
3.2.6	<i>Virtual Disk</i>	99
3.3	ACCESS RIGHT MANAGEMENT	101
3.3.1	<i>Users</i>	101
3.3.2	<i>User Groups</i>	107
3.3.3	<i>Share Folders</i>	108
3.3.3.1	<i>Share Folder</i>	108
3.3.3.2	<i>Folder Aggregation</i>	109
3.3.4	<i>Quota</i>	113
3.4	NETWORK SERVICES	114
3.4.1	<i>Microsoft Networking</i>	114
3.4.2	<i>Apple Networking</i>	116
3.4.3	<i>NFS Service</i>	116
3.4.4	<i>FTP Service</i>	117
3.4.5	<i>Telnet/SSH</i>	119
3.4.6	<i>SNMP Settings</i>	120
3.4.7	<i>Web Server</i>	122
3.4.7.1	<i>WebDAV</i>	124
3.4.8	<i>Network Service Discovery</i>	144
3.4.8.1	<i>UPnP Discovery Service</i>	144
3.4.8.2	<i>Bonjour</i>	145
3.5	APPLICATIONS	146
3.5.1	<i>Web File Manager</i>	146
3.5.2	<i>Multimedia Station</i>	147
3.5.3	<i>Download Station</i>	147
3.5.4	<i>Surveillance Station</i>	148
3.5.5	<i>iTunes Service</i>	156

3.5.6	UPnP Media Server.....	159
3.5.7	MySQL Server.....	161
3.5.8	QPKG Plugins.....	163
3.6	BACKUP.....	164
3.6.1	External Drive.....	164
3.6.2	USB One Touch Copy.....	166
3.6.3	Remote Replication.....	167
3.6.3.1	Remote Replication.....	167
3.6.3.2	Amazon S3.....	173
3.6.4	Time Machine.....	175
3.7	EXTERNAL DEVICE.....	179
3.7.1	External Storage Device.....	179
3.7.2	USB Printer.....	180
3.7.2.1	Windows XP Users.....	181
3.7.2.2	Windows Vista/ Windows 7 Users.....	183
3.7.2.3	Mac OS X 10.4.....	185
3.7.2.4	Mac OS X 10.5.....	189
3.7.3	UPS Settings.....	195
3.8	SYSTEM STATUS.....	198
3.8.1	System Information.....	198
3.8.2	System Service.....	199
3.8.3	Resource Monitor.....	200
CHAPTER 4	MULTIMEDIA STATION.....	201
CHAPTER 5	DOWNLOAD STATION.....	209
5.1	USE DOWNLOAD SOFTWARE QGET.....	217
CHAPTER 6	WEB FILE MANAGER.....	219
CHAPTER 7	NETBAK REPLICATOR.....	223
CHAPTER 8	ACTIVE DIRECTORY.....	238
CHAPTER 9	NAS MAINTENANCE.....	246
9.1	RESTART/ SHUT DOWN SERVER.....	246
9.2	RESET ADMINISTRATOR PASSWORD AND NETWORK SETTINGS.....	248
9.3	DISK FAILURE OR MALFUNCTION.....	250
9.4	POWER OUTAGE OR ABNORMAL SHUTDOWN.....	250
9.5	SYSTEM SOFTWARE ABNORMAL OPERATION.....	250
9.6	SYSTEM TEMPERATURE PROTECTION.....	251

CHAPTER 10	RAID OPERATION TROUBLESHOOTING	252
CHAPTER 11	USE THE LCD PANEL.....	254
APPENDIX A.	CONNECT TO QNAP NAS FROM THE INTERNET.....	261
APPENDIX B.	SET SMS AND EMAIL ALERT.....	269
APPENDIX C.	ONLINE RAID CAPACITY EXPANSION & ONLINE RAID LEVEL	
MIGRATION	278
APPENDIX D.	SET UP UPNP MEDIA SERVER FOR MEDIA PLAYING	290
APPENDIX E.	HOST A FORUM WITH PHPBB ON QNAP NAS	298
TECHNICAL SUPPORT.....		309
GNU GENERAL PUBLIC LICENSE		310

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 the server's normal operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disk drives (HDD) in the NAS when installing the HDD for proper operation.
7. Do not place the NAS near any liquid.
8. Do not place the NAS on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using the NAS. If you are not sure, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair your NAS in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.
12. The chassis (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.

Chapter 1 Install the NAS

For the information of hardware installation, see the 'Quick Installation Guide' in the product package.

1.1 Hard Disk Drive Compatibility List

This product works with 2.5-inch/ 3.5-inch SATA hard disk drives (HDD) from major HDD brands. For the HDD 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 HDD (new or used) which has never been installed on the NAS before, the HDD will be formatted and partitioned automatically and all the disk data will be cleared.

1.2 Check System Status

LED Display & System Status Overview

LED	Colour	LED Status	Description
USB	Blue	Flashes blue every 0.5 sec	<ol style="list-style-type: none"> 1) A USB device (connected to front USB port) is detected 2) A USB device (connected to front USB port) is 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 the eSATA device
		Blue	<ol style="list-style-type: none"> 1) A front USB device is detected (after the device is mounted) 2) The NAS has finished copying the data to or from the USB device connected to the front USB port
		Off	No USB device can be detected
eSATA*	Orange	Flashes	The eSATA device is being accessed
		Off	No eSATA device can be detected
System Status	Red/ Green	Flashes green and red alternately every 0.5 sec	<ol style="list-style-type: none"> 1) The HDD on the NAS is being formatted 2) The NAS is being initialised 3) The system firmware is being updated 4) RAID rebuilding is in process 5) Online RAID capacity expansion is in process 6) Online RAID level migration is in process

		Red	<ol style="list-style-type: none"> 1) The HDD 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 HDD 7) The NAS is in degraded read-only mode (2 member HDD fail in a RAID 5 or RAID 6 configuration, the disk data can still be read) 8) (Hardware self-test error)
System Status	Red/ Green	Flashes red every 0.5 sec	The NAS is in degraded mode (one member HDD 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 HDD is not formatted
		Green	The NAS is ready
		Off	All the HDD on the NAS are in standby mode
HDD	Red/ Green	Flashes red	The disk data is being accessed and a read/ write error occurs during the process
		Red	A HDD read/ write error occurs
		Flashes green	The disk data is being accessed
		Green	The HDD can be accessed
LAN	Orange	Orange	The NAS is connected to the network
		Flashes orange	The NAS is being accessed from the network

* TS-210, TS-219, TS-439U-SP/RP, TS-809 Pro, TS-809U-RP do not support eSATA port.

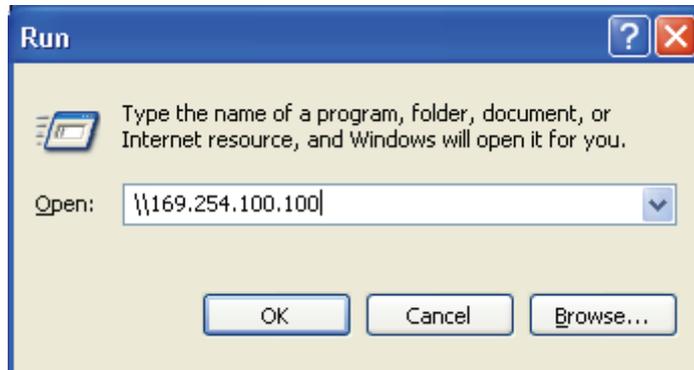
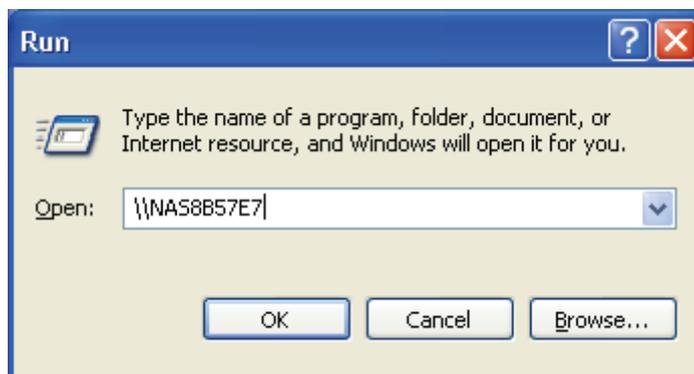
Beep Alarm (beep alarm can be disabled in 'System Tools' > 'Hardware Settings')

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 HDD on the NAS are in degraded mode 4) The user starts HDD 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

Chapter 2 Connect to the NAS

Windows Users

1. You can 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 you cannot find the server, browse the whole network to search for the NAS. Double click the name of the NAS for connection.
 - b. Use the Run function in Windows. Enter **\\NAS name** or **\\NAS IP**



2. Enter the default administrator name and password.

Default user name: admin
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_nameFor 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 your NAS is 192.168.0.1 and you want to link the network share folder 'public' under the /mnt/pub directory, use the following command:

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

Note: You must login as 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.

Access the NAS by web browser on Windows or Mac

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

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

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



3. You can browse the NAS UI by the Standard view or the Flow view.

Standard view:



Flow view:



- To configure the NAS, click 'ADMINISTRATION'. Enter the administrator name and password.

Default administrator name: **admin**
Password: **admin**

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



- You can turn on the option 'SSL login' (Secure Sockets Layer login) to allow secure connection to the NAS.

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

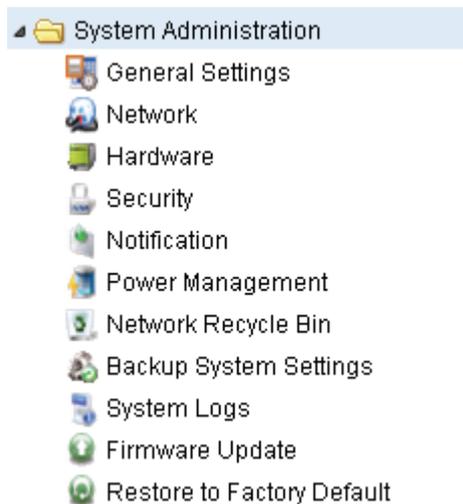
User Name: admin
Password: ●●●●●●
 Remember user name
 Remember password
 SSL login
SUBMIT CANCEL

Chapter 3 Server Administration

There are 8 sections in the server administration.



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



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

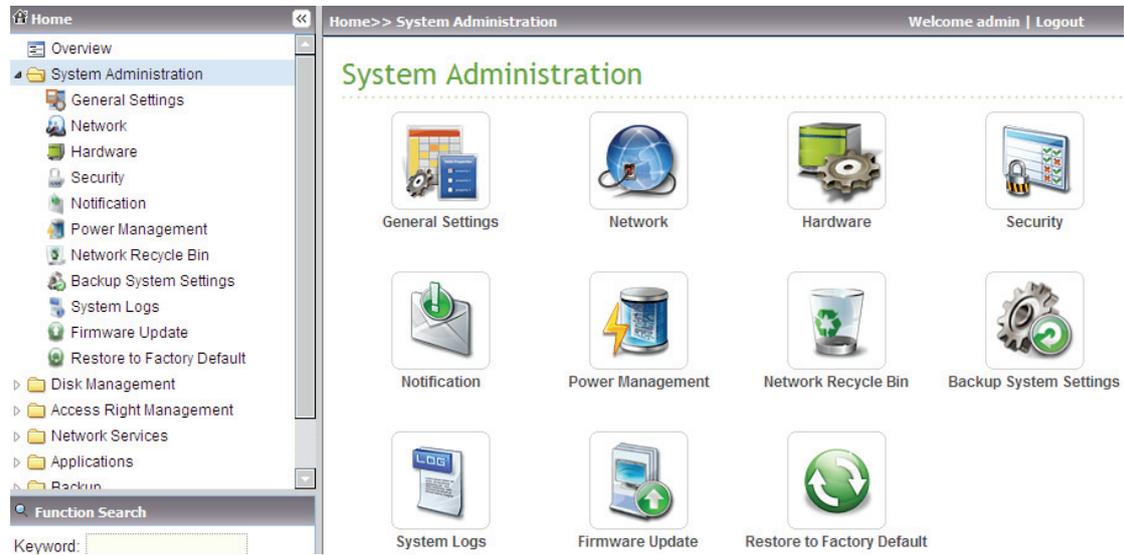


After you login the NAS, you can click the icons on top of the page to access the services.

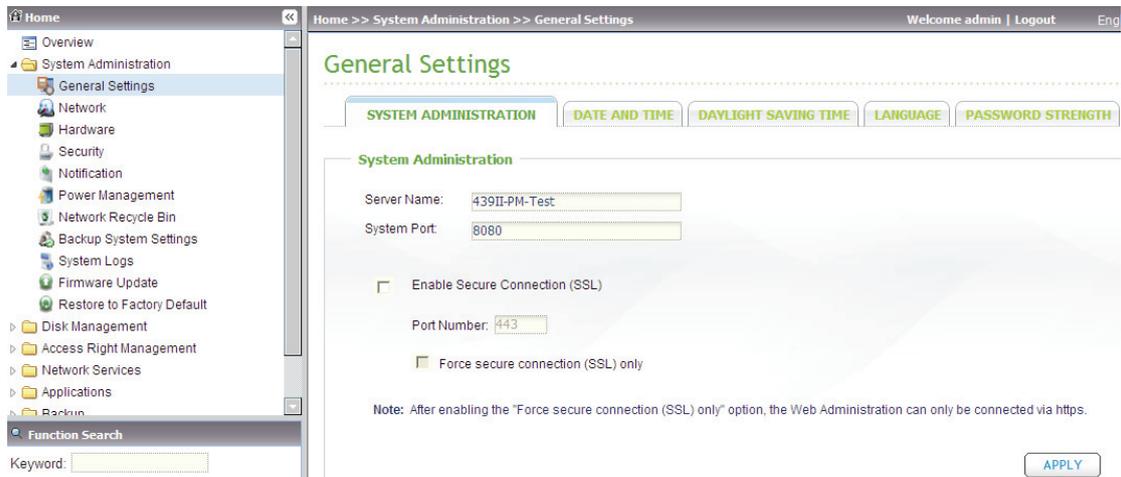


3.1 System Administration

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



3.1.1 General Settings



3.1.1.1 System Administration

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

Assign a port for the system management. The default port is 8080. The services which use this port include: System Management, Web File Manager, Multimedia Station, and Download Station. 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 you turn on the option 'Force secure connection (SSL) only', the users can only connect to the web administration page by https connection.

3.1.1.2 Date and Time

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

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

✓ Synchronize with an Internet time server automatically

You can turn on this option to synchronize the date and time of the NAS automatically with specified 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.

The screenshot shows a web interface for configuring the Date and Time settings. At the top, there are five tabs: SYSTEM ADMINISTRATION, DATE AND TIME (selected), DAYLIGHT SAVING TIME, LANGUAGE, and PASSWORD STRENGTH. Below the tabs, the 'Date and Time' section is visible. It includes a 'Time Zone' dropdown menu set to '(GMT+08:00) Taipei'. The 'Date/Time' section shows a date of 2010/4/20, time of 15:52:17, and a 24HR interval. The 'Date Format' is set to yyyy/MM/DD. There are two 'UPDATE NOW' buttons. The first is for setting the server time to match the computer time. The second is for synchronizing with an internet time server automatically, which is currently unchecked. The 'Server' field is set to pool.ntp.org. The 'Time Interval' is set to 1 day(s). An 'APPLY' button is located at the bottom right.

3.1.1.3 Daylight Saving Time

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

The system time will be adjusted automatically according to the DST.

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

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="checkbox"/>				<input type="button" value="Delete"/>

3.1.1.4 Language

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

Note: All files and directories on the NAS will be created using Unicode encoding.

If the FTP clients or the OS of your PC does not support Unicode, select the language which is the same as your OS language in order to view the files and directories on the server properly.

The screenshot shows a navigation bar with five tabs: SYSTEM ADMINISTRATION, DATE AND TIME, DAYLIGHT SAVING TIME, LANGUAGE, and PASSWORD STRENGTH. The LANGUAGE tab is selected and highlighted. Below the navigation bar, the page title is "Language". Underneath, there is a label "Filename Encoding:" followed by a dropdown menu currently set to "English". At the bottom right of the configuration area, there is an "APPLY" button.

3.1.1.5 Password Strength

You can specify the password rules. After applying the setting, the NAS will automatically check the validity of the password.

The screenshot shows a navigation bar with five tabs: SYSTEM ADMINISTRATION, DATE AND TIME, DAYLIGHT SAVING TIME, LANGUAGE, and PASSWORD STRENGTH. The PASSWORD STRENGTH tab is selected and highlighted. Below the navigation bar, the page title is "Password Strength". Underneath, there are three checkboxes, each followed by a numbered rule:

- 1. The new password contains characters from at least three of the following classes: lower case 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.

At the bottom right of the configuration area, there is an "APPLY" button.

3.1.2 Network

3.1.2.1 TCP/IP

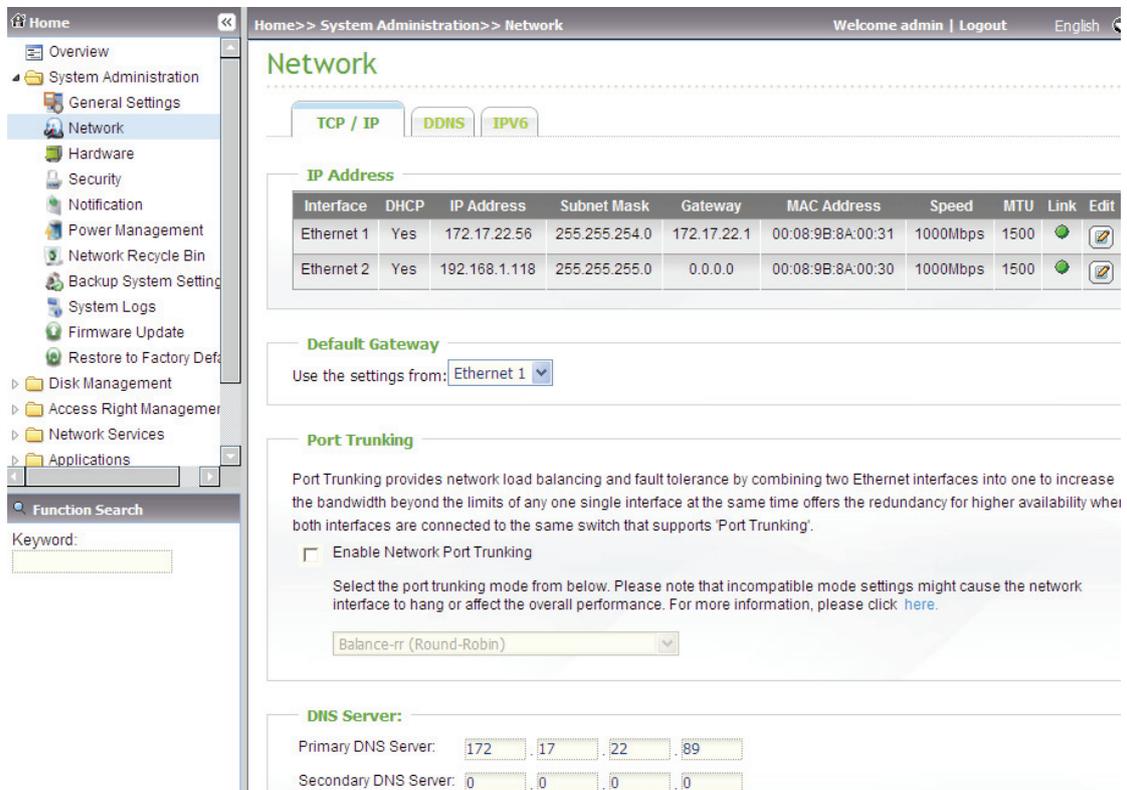
i. IP Address

You can configure the TCP/IP settings of the NAS on this page. Click the Edit button

() to edit the network settings.

For the NAS which supports two LAN ports, you can connect both network interfaces to two different switches and configure the TCP/IP settings. The NAS will acquire two IP addresses which allow the access from two different subnets. This is known as multi-IP setting*. When using Finder to detect the NAS IP, the IP of Ethernet 1 will be shown in LAN 1 only and the IP of 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, and TS-219P provide one Giga LAN port only therefore do not support dual LAN configuration or port trunking.



The screenshot shows the Network configuration page in the NAS web interface. The page is titled "Network" and has tabs for "TCP / IP", "DDNS", and "IPV6". The "TCP / IP" tab is selected. 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	Yes	172.17.22.56	255.255.254.0	172.17.22.1	00:08:9B:8A:00:31	1000Mbps	1500		
Ethernet 2	Yes	192.168.1.118	255.255.255.0	0.0.0.0	00:08:9B:8A:00:30	1000Mbps	1500		

The "Default Gateway" section shows "Use the settings from:" with a dropdown menu set to "Ethernet 1". The "Port Trunking" section has a checkbox for "Enable Network Port Trunking" which is unchecked. Below it, a dropdown menu is set to "Balance-rr (Round-Robin)". The "DNS Server" section has input fields for "Primary DNS Server" (172, 17, 22, 89) and "Secondary DNS Server" (0, 0, 0, 0).

TCP/IP - Property

Network Speed: Auto-negotiation

Obtain IP address settings automatically via DHCP

Use static IP address

Fixed IP Address: 169 . 254 . 100 . 100

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 169 . 254 . 100 . 100

Enable DHCP Server

Start IP Address: 169 . 254 . 1 . 100

End IP Address: 169 . 254 . 1 . 200

Lease Time: 1 Day 0 Hour

Step 1 of 1

APPLY CANCEL

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 your 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.

- **Enable DHCP Server**

If no DHCP is available on the LAN where the NAS locates, you can turn on this function to make the NAS a DHCP server. The NAS will allocate dynamic IP address to the DHCP clients on the LAN.

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

clients by the DHCP server. When the lease time expires, the client has to acquire an IP address from the DHCP server again.

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

This option is available to Ethernet 1 only when both LAN ports of the dual LAN NAS are connected to the network.

ii. Default Gateway

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

— **Default Gateway** —

Use the settings from: 





iii. Port Trunking

Applicable to NAS models with two LAN ports only. This feature is not supported by TS-110, TS-119, TS-210, TS-219, and TS-219P.

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 both LAN ports of the NAS are connected to the same switch and you have configured the settings described in sections (i) and (ii).

Follow the steps below to configure port trunking on the NAS:

1. Select the option 'Enable Network Port Trunking'.
2. Choose a port trunking mode from the drop-down menu. The default option is Active Backup (Failover).

Port Trunking

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

Enable Network Port Trunking

Select the port trunking mode from below. Please note that incompatible mode settings might cause the interface to hang or affect the overall performance. For more information, please click [here](#).

- Active Backup(Fail Over)
- Balance-rr (Round-Robin)
- Active Backup(Fail Over)
- Balance XOR
- Broadcast
- IEEE 802.3ad
- Balance-tlb (Adaptive Transmit Load Balancing)
- Balance-alb (Adaptive Load Balancing)

3. Click 'Apply'.
4. The Ethernet interfaces will be combined as Ethernet 1+2. Click the Edit button () to edit the network settings.

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1+2	No	10.8.13.2	255.255.254.0	10.8.12.1	00:08:9B:BE:23:DA	100Mbps	1500		

- After applying the settings, make sure the network cables of the two Ethernet interfaces are connected to the correct switch and the switch has been configured to support the port trunking mode selected on the NAS.

Refer to the table below about 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 maybe selected via the	Supports static trunking. Make sure static trunking is enabled on the switch.

	xmit_hash_policy option. Balance XOR mode provides load balancing and fault tolerance.	
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	General switches

	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.	
--	--	--

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:

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

v. 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 your network appliances support Jumbo Frame setting, select the appropriate MTU value for your network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.

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

3.1.2.2 DDNS

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

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

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 [Appendix A](#).

TCP / IP DDNS IPV6

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

User Name:

Password:

Host Name:

Check the External IP Address Automatically

Current WAN IP: 219.85.63.13

Recent DDNS Update Result

Connection IP Last Checked:

Next Check for Connection IP:

Last DDNS Update Time:

Update Server Response:

APPLY

3.1.2.3 IPv6

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

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

TCP / IP DDNS IPv6

IP Address

Enable IPv6

Interface	Auto Configuration	IPv6 Address	Prefix Length	Gateway	Link	Edit
-----------	--------------------	--------------	---------------	---------	------	------

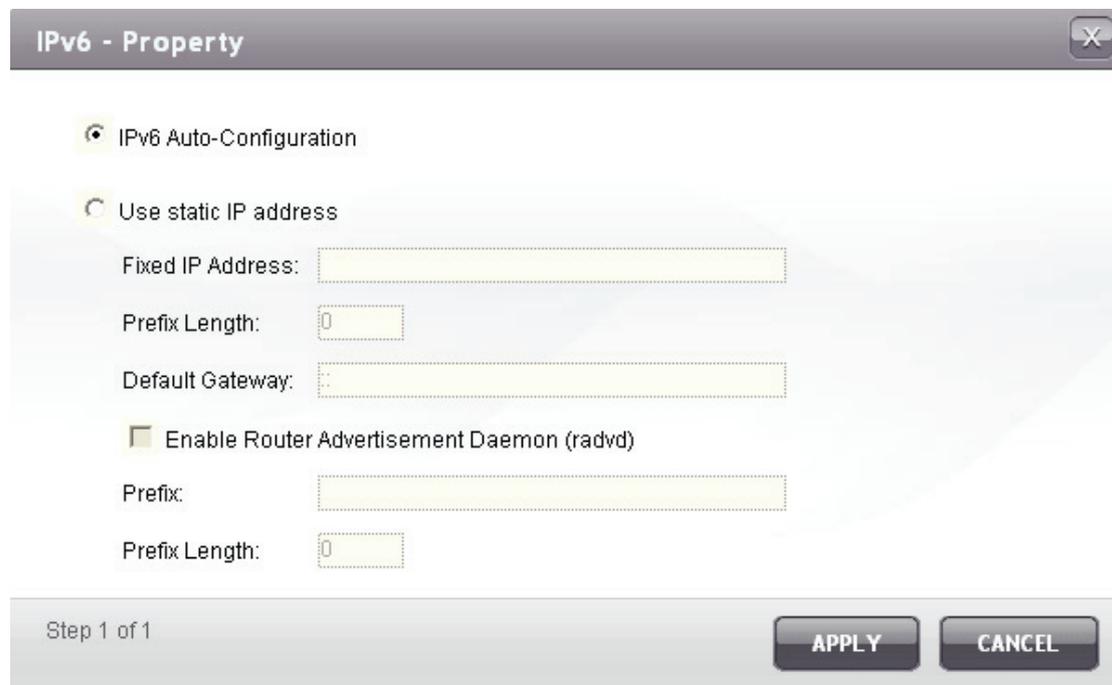
DNS Server:

.....

.....

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

- **Use static IP address**

To use a static IP address, enter the IP address (for example, 2001:bc95:1234:5678), prefix length (for example, 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)**

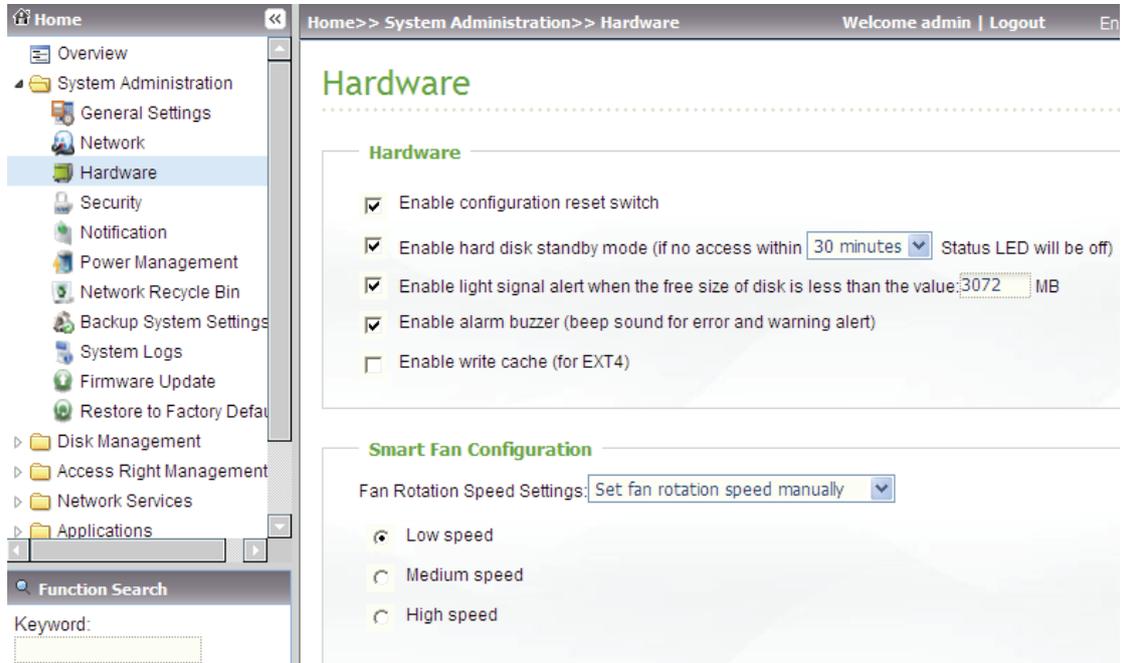
To configure the NAS as an IPv6 host and distribute IPv6 addresses to the local clients which support IPv6, turn on this option and enter the prefix and prefix length.

- **IPv6 DNS server**

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

3.1.3 Hardware

You can set the hardware functions of the NAS.



- Enable configuration reset switch
When this function is turned on, you can press the reset button for 3 seconds to reset the administrator password and the system settings to default. The disk data will be retained.
- Enable hard disk standby mode
When this function is turned on, the HDD enters standby mode if there is no access within the specified period.
- Enable light signal alert when the free size of SATA disk is less than the value:
The status LED flashes red and green when this function is turned on and the free space of the SATA HDD is less than the value. The range of the value is 1-51200 MB.
- Enable alarm buzzer
Enable this option and the NAS will sound when an error occurs.
- Enable write cache (for EXT4)
If the disk volume of the NAS is in EXT 4 format, you can gain better write performance by turning on this option. 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.

- Smart fan configuration

- (i) Enable smart fan (recommended)

Select to use the default smart fan settings or define the settings manually.

When the system default settings are selected, the fan rotation speed is automatically adjusted when the server temperature, CPU temperature, and HDD temperature meet the criteria. It is recommended to turn on 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 you have installed two power supply units (PSU) on the NAS and connected them to the power sockets, both PSU will supply the power to the NAS (applied to 1U and 2U models). You can turn on 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 you have installed only one PSU on the NAS, you are suggested NOT to enable this option.

* This function is disabled by default.

Hardware

Hardware

- Enable configuration reset switch
- Enable hard disk standby mode (if no access within Status LED will be off)
- Enable light signal alert when the free size of disk is less than the value: MB
- Enable alarm buzzer (beep sound for error and warning alert)
- Enable Redundant Power Supply Mode

3.1.4 Security

3.1.4.1 Security Level

Enter the IP address or network domain from which the connections to this server 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 local server.

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

The screenshot shows a web management interface for system administration. The left sidebar contains a navigation menu with categories like System Administration, Network, Hardware, Security, Notification, Power Management, Network Recycle Bin, Backup System Settings, System Logs, Firmware Update, Restore to Factory Default, Disk Management, Access Right Management, Network Services, Applications, and Backup. The 'Security' option is selected. The main content area is titled 'Security' and has three tabs: 'SECURITY LEVEL', 'NETWORK ACCESS PROTECTION', and 'IMPORT SSL SECURE CERTIFICATE'. The 'SECURITY LEVEL' tab is active, showing three radio button options: 'High: Allow connections from the list only', 'Medium: Deny connections from the list', and 'Low: Allow all connections'. Below these options is a text input field for entering IP addresses or network domains, with '+' and '-' buttons for adding or removing entries. At the bottom, there is a table with three columns: 'Genre', 'IP address or network domain', and 'Time left for IP blocking'. The table is currently empty.

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

3.1.4.2 Network Access Protection

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

SECURITY LEVEL **NETWORK ACCESS PROTECTION** **IMPORT SSL SECURE CERTIFICATE**

Network Access Protection

Enable network access protection

SSH: In , after unsuccessful attempts for , block the IP for

Telnet: In , after unsuccessful attempts for , block the IP for

HTTP(S): In , after unsuccessful attempts for , block the IP for

FTP: In , after unsuccessful attempts for , block the IP for

SAMBA: In , after unsuccessful attempts for , block the IP for

AFP: In , after unsuccessful attempts for , block the IP for

3.1.4.3 Import SSL Secure Certificate

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

SECURITY LEVELNETWORK ACCESS PROTECTIONIMPORT SSL SECURE CERTIFICATE

Import SSL Secure Certificate

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: Default secure certificate being used

Certificate: Please enter a certificate in X.509PEM format below. [View sample](#)

Private Key: Please enter a certificate or private key in X.509PEM format below. [View sample](#)

CLEARUPLOAD

3.1.5 Notification

3.1.5.1 Configure SMTP Server

The NAS supports email alert to inform you 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 the message is sent.
- User Name and Password: Enter the login information of your email account, for example, your Gmail login name and password.
- Use SSL/ TLS secure connection: If the SMTP server supports this function, you can turn it on.

Home >> System Administration >> Notification Welcome

Notification

[CONFIGURE SMTP SERVER](#) [CONFIGURE SMSC SERVER](#) [ALERT NOTIFICATION](#)

Configure SMTP Server

SMTP Server:

Port Number:

Sender:

Enable SMTP Authentication

User Name:

Password:

Use SSL/ TLS secure connection

3.1.5.2 Configure SMSC Server

You can configure SMS server settings to send SMS messages 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 you select 'Add SMS service provider', enter the name of the SMS provider and the URL template text.

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

CONFIGURE SMTP SERVER **CONFIGURE SMSC SERVER** **ALERT 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: <http://www.clickatell.com>

Enable SSL Connection

SSL Port:

SMS Server Login Name:

SMS Server Login Password:

SMS Server API_ID:

APPLY

3.1.5.3 Alert Notification

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

For more information, see [Appendix B](#).

CONFIGURE SMTP SERVERCONFIGURE SMSC SERVERALERT NOTIFICATION

Alert Notification

When a system event occurs, an alert email/SMS will be sent automatically.

Send system error alert by: No alert ▼

Send system warning alert by: No alert ▼

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.

SMS Notification Settings

Country Code: Afghanistan (+93) ▼

Cell Phone No. 1: +93

Cell Phone No. 2: +93

SEND A TEST SMS MESSAGE

Note: You must configure the SMSC server to be able to send SMS notification properly.

APPLY

3.1.6 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 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.

- **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 not supported by TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, and TS-419U.

- **Power resumption settings**

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

- **Power on/ power off/ restart schedule**

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

Home >> System Administration >> Power Management

Welcome admin | Logout English

Power Management

Restart/ Shutdown

Execute system restart/ shutdown immediately.

Configure Wake on LAN

Enable
 Disable

When the AC power resumes:

Resume the server to the previous power-on or power-off status.
 Turn on the server automatically.
 The server should remain off.

Set power on/ power off/ restart schedule

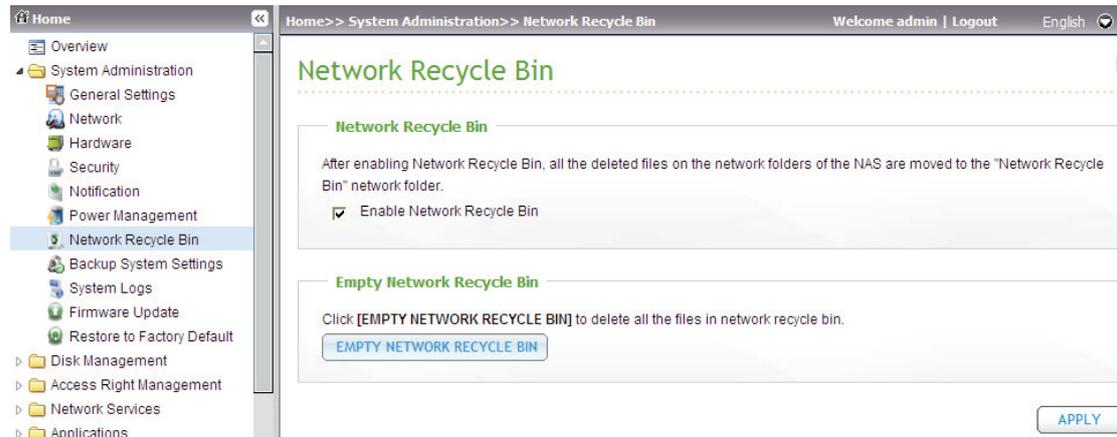
Enable schedule
 Postpone the restart/shutdown schedule when a replication job is in progress.

Shutdown | Daily | 7 | 0

3.1.7 Network Recycle Bin

This function enables the files deleted on the shares of the NAS to be removed to Network Recycle Bin to reserve the files temporarily. To turn on this function, select the option 'Enable Network Recycle Bin' and click 'Apply'. The NAS will create a network share named 'Network Recycle Bin' automatically.

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



3.1.8 Back up/ Restore 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.

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

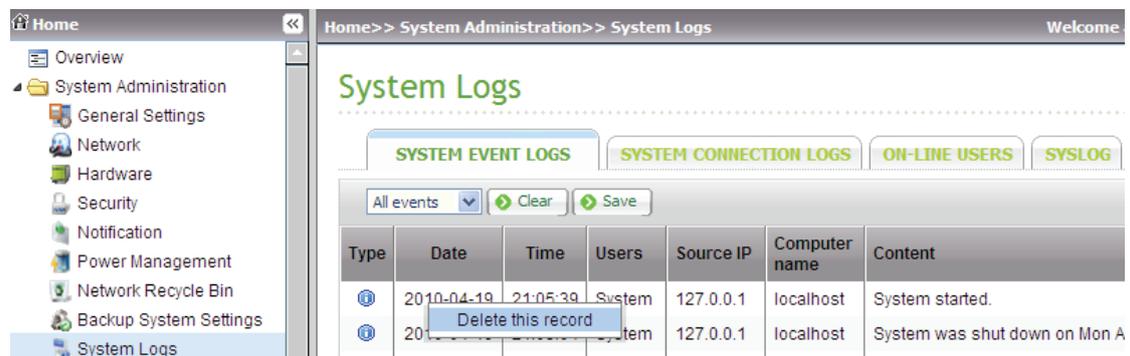


3.1.9 System Logs

3.1.9.1 System Event Logs

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

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



The screenshot shows a web-based interface for System Administration. The left sidebar contains a navigation menu with items like Overview, System Administration, General Settings, Network, Hardware, Security, Notification, Power Management, Network Recycle Bin, Backup System Settings, and System Logs. The main content area is titled 'System Logs' and features four tabs: SYSTEM EVENT LOGS (selected), SYSTEM CONNECTION LOGS, ON-LINE USERS, and SYSLOG. Below the tabs is a filter dropdown set to 'All events', and buttons for 'Clear' and 'Save'. A table displays the log entries with columns for Type, Date, Time, Users, Source IP, Computer name, and Content. A context menu is open over the second row, showing a 'Delete this record' option.

Type	Date	Time	Users	Source IP	Computer name	Content
Information	2010-04-19	21:05:39	System	127.0.0.1	localhost	System started.
Information	2010-04-19	21:05:39	System	127.0.0.1	localhost	System was shut down on Mon A

3.1.9.2 System Connection Logs

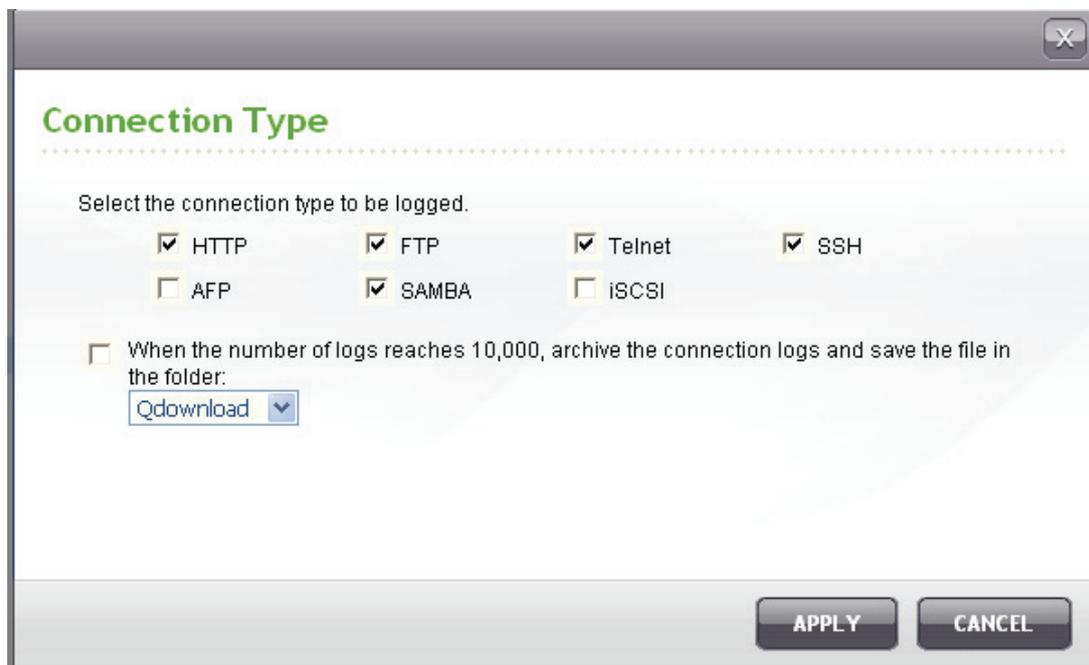
The NAS supports recording HTTP, FTP, Telnet, SSH, AFP, NFS, SAMBA, and iSCSI connections. Click 'Options' to select the connection type to be logged.

The file transfer performance can be slightly affected when this feature is turned on.

Tip: You can right click a log and select to delete the record or block the IP and select how long the IP should be blocked.



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.



3.1.9.3 On-line Users

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

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

System Logs

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

Type	Login date	Login time	Users	Source IP	Computer name	Connection type	Accessed resources
	2010-04-20	15:41:24				pa	Qdownload
	2010-04-20	15:39:40				pa	Qdownload
	2010-04-19	21:08:26				pa	Qusb
	2010-04-20	15:24:15	admin	10.8.12.44	---	HTTP	Administration
	2010-04-20	11:16:52	admin	10.8.12.43	---	HTTP	Administration

There are 5 events.

3.1.9.4 Syslog

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

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:

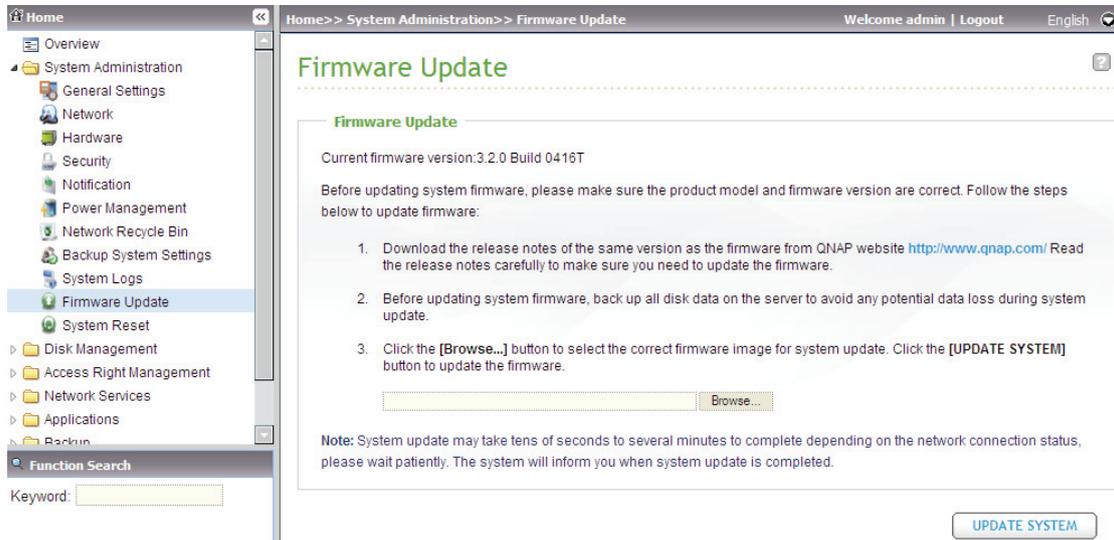
Select the logs to record

System Event Logs

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

APPLY

3.1.10 Firmware Update



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

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

Step 1: Download the release notes of the firmware from the QNAP website <http://www.qnap.com>. Read the release notes carefully to make sure you need to update the firmware.

Step 2: Download the NAS firmware and unzip the IMG file to your computer.

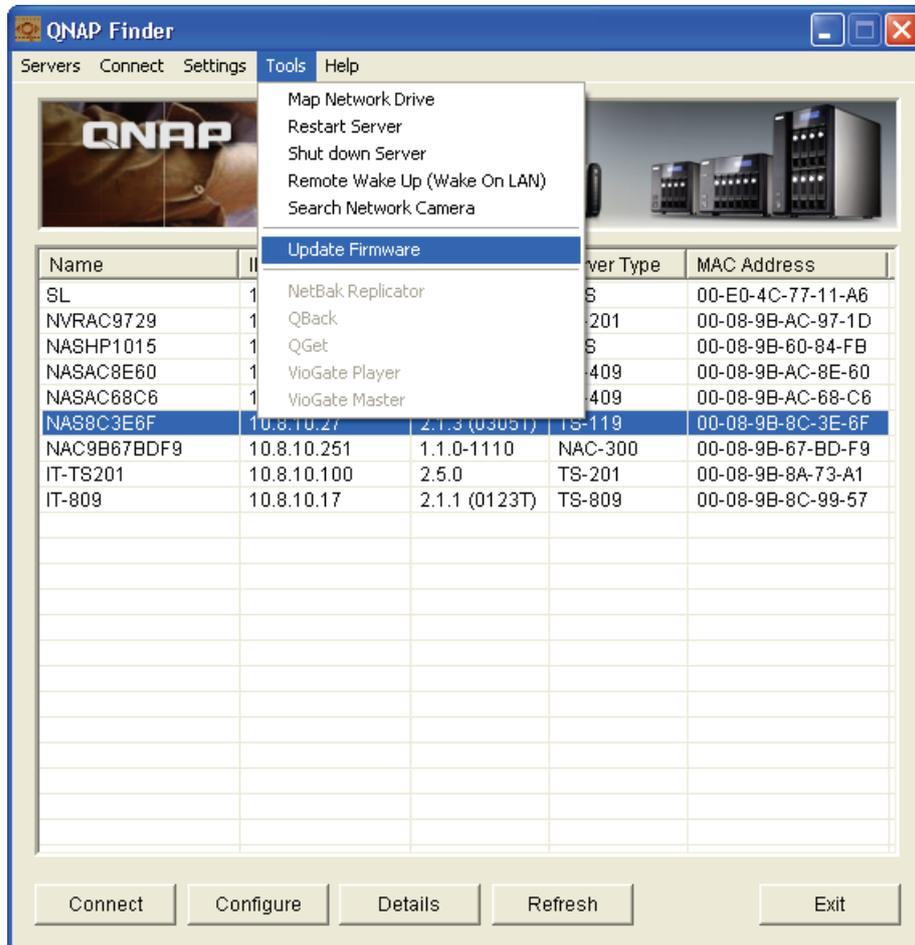
Step 3: Before updating the system firmware, back up all the disk data on the server to avoid any potential data loss during the system update.

Step 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 the system firmware by Finder

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



Login the NAS as a user with administrator access right.



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

Select the system firmware to be installed or updated to the system hard disk.

Path of system firmware image file:
C:\Documents and Settings\Administrator\Desktop\TS-119_20090313-2.1.4.i

Firmware Model: TS-119, Version: 2.1.4.

Server Name	Model Name	Version	MAC Address	Pro...	Status
<input checked="" type="checkbox"/> NAS8C3E6F	TS-119	2.1.3 (0305T)	00-08-9B-8C-3E-6F		

Update all the servers with the same model number within the network

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

3.1.11 Restore to Factory Default

To reset all the settings to default, click 'RESET'.



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



3.2 Disk Management



3.2.1 Volume Management

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

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

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

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

Home >> Disk Management >> Volume Management Welcome admin | Logout English

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.



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).



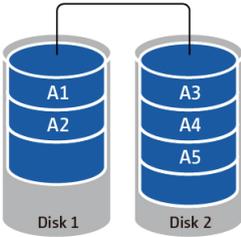
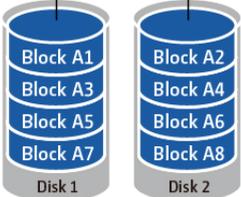
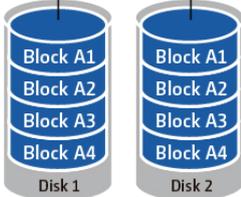
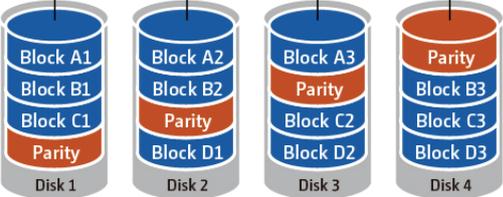
RAID 6 Disk Volume
Combine 4 or more disks to create a disk volume with data protection (2 failed disks are allowed).

Current Disk Volume Configuration: Physical Disks					
Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	WDC WD7500AADS-22M2B01.0	698.64 GB	Ready	SCAN NOW	GOOD
Drive 2	--	--	No Disk	SCAN NOW	---
Drive 3	--	--	No Disk	SCAN NOW	---
Drive 4	--	--	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.

Current Disk Volume Configuration: Logical Volumes				
Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 1	EXT4	686.20 GB	685.76 GB	Ready

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

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

minimum of 3 HDD are required.

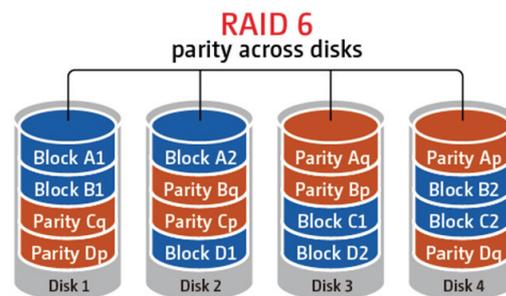
The storage capacity of a RAID 5 array equals $(N-1)$. N is the total number of HDD members in the array.

RAID 6 Disk Volume

The data are striped across all the HDD 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 drives HDD.

To create a RAID 6 disk volume, a minimum of 4 hard disks are required.

The storage capacity of a RAID 6 array equals $(N-2)$. N is the total number of HDD members in the array.



3.2.2 RAID Management

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

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

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

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

RAID Recovery: When the NAS is configured as RAID 5 (or RAID 6) and 2 (or 3) HDD are unplugged from the server accidentally, you can plug in the same HDD 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 HDD members are disconnected, you can use this function to recover the volume status from 'Not active' to 'Normal'. The disk volume can be used normally after successful recovery.

Note: If the disconnected drive member is damaged, the RAID recovery function will not work.

For more information about online RAID capacity expansion and online RAID level migration, see [Appendix C](#).

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
Mirroring Disk Volume: Drive 1 2	456.98 GB	Yes	Ready	The operation(s) you can execute: - Expand capacity
<div style="display: flex; justify-content: space-between; align-items: center;"> EXPAND CAPACITY ADD HARD DRIVE MIGRATE CONFIGURE SPARE DRIVE DISABLE BITMAP RECOVER </div>				

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

RAID Level \ RAID Status	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 & HDD replacement)	N/A	N-1, bad blocks found in the surviving HDD of the array.	N/A	N-2, bad blocks found in the surviving HDD of the array.
RAID Recovery (RAID Status: Not Active)	N/A	If re-plugging in all original HDD to the NAS and they can be spun up, identified, accessed, and the HDD superblock is not damaged.	N/A	If re-plugging in all original HDD to the NAS and they can be spun up, identified, accessed, and the HDD superblock is not damaged).
RAID Crash	N-2	N-2 failed HDD and any of the remaining HDD cannot be spun up/ identified/ accessed.	N-3	N-3 and any of the remaining HDD cannot be spun up/ identified/ accessed.

N = Number of hard disk drives (HDD) in the array

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

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

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

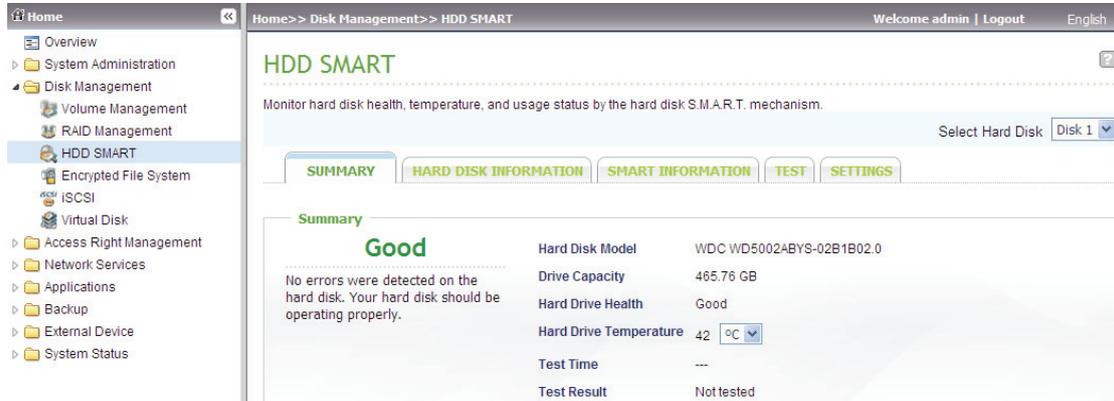
Single * 1	6	Online RAID level migration	RAID 6 * 7
Single * 1	7	Online RAID level migration	RAID 6 * 8
RAID 1 * 2	1	Online RAID level migration	RAID 5 * 3
RAID 1 * 2	2	Online RAID level migration	RAID 5 * 4
RAID 1 * 2	3	Online RAID level migration	RAID 5 * 5
RAID 1 * 2	4	Online RAID level migration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

3.2.3 HDD SMART

You can monitor the HDD health, temperature, and the usage status by HDD S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology).

You can view the following information of each HDD on the NAS.

Field	Description
Summary	Display the HDD S.M.A.R.T. summary and the latest test result.
Hard disk information	Display the HDD details, for example, model, serial number, HDD capacity.
SMART information	Display the HDD 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 HDD S.M.A.R.T. test.
Settings	Configure temperature alarm. When the HDD 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.



3.2.4 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, and TS-419U.

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

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

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

Encryption Key Management

Volume	Total Size	Status	Action
RAID 5 Disk Volume: Drive 1 2 3	455.52 GB	Unlocked	ENCRYPTION KEY MANAGEMENT

3.2.5 iSCSI

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

3.2.5.1 *iSCSI Target*

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

1. Install an iSCSI initiator on your computer (Windows PC, Mac, or Linux).
2. Enable iSCSI Target Service on the NAS and create a new 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 your computer.

In between the relationship of your computer and the storage device, your 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 or Intel-based NAS models running firmware prior to version 3.2.0 only.

Non Intel-based NAS refers to TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, TS-419U. Intel-based NAS refers to TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, and TS-809U-RP.

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.

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



Enter the information required. Specify 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.

Create New iSCSI Target

iSCSI Target Profile

Target Name:

iSCSI Target IQN: iqn.2004-04.com.qnap.ts-219:iscsi.mytarget.8cdd00

iSCSI Target LUN

Allocate the disk space now ?

Volume:

Free Size:913GB

Capacity: GB

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

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

Field	User name limitation	Password limitation
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

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

iSCSI Configuration

ISCSI TARGET | **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	  

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

PORTAL MANAGEMENT | **TARGET MANAGEMENT**

iSCSI Portal

Enable iSCSI Target Service

iSCSI Service Port:

Enable iSNS

iSNS Server IP:

APPLY

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

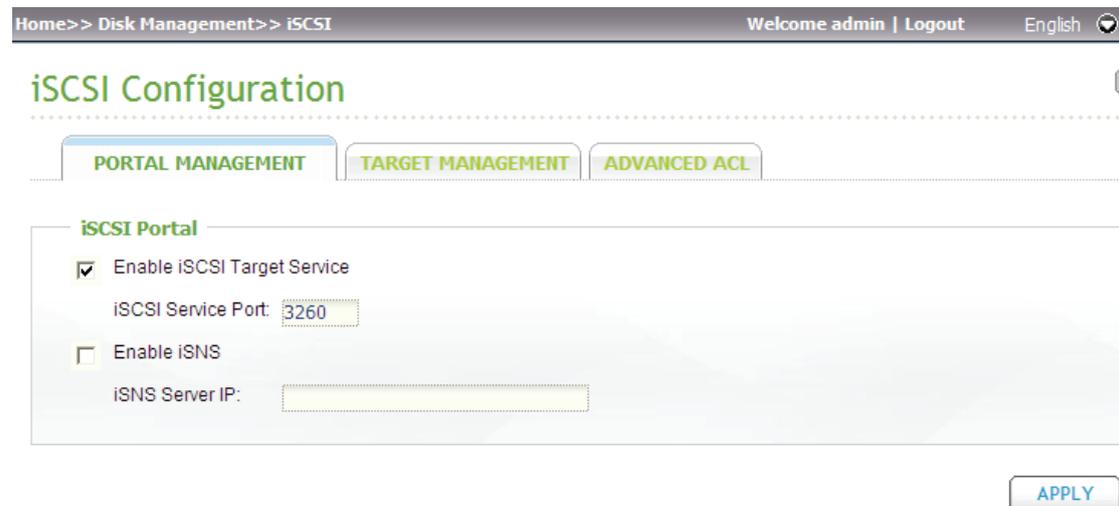
Intel-based NAS refers to TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, and TS-809U-RP.

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 your network infrastructure and the application performance. Too many concurrent connections may slow down the performance of the NAS.

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

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



2. Next, 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 select the options 'Data Digest' and '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. The main content area is titled 'Create New iSCSI Target' in green. On the left side, there is a logo for 'QNAP TURBO NAS'. The configuration fields are as follows:

- iSCSI Target Profile**
 - Target Name:
 - iSCSI Target IQN:
 - Target Alias:
- CRC/Checksum (optional)**
 - Data Digest
 - Header Digest

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

- Enter the CHAP authentication settings. If you enter the user name and password settings under 'Use CHAP authentication' only, only the iSCSI target authenticates the initiator. In other words, the initiators have to enter the user name password settings to connect to the target.

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

Field	User name limitation	Password limitation
Use CHAP authentication	<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
✕



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:

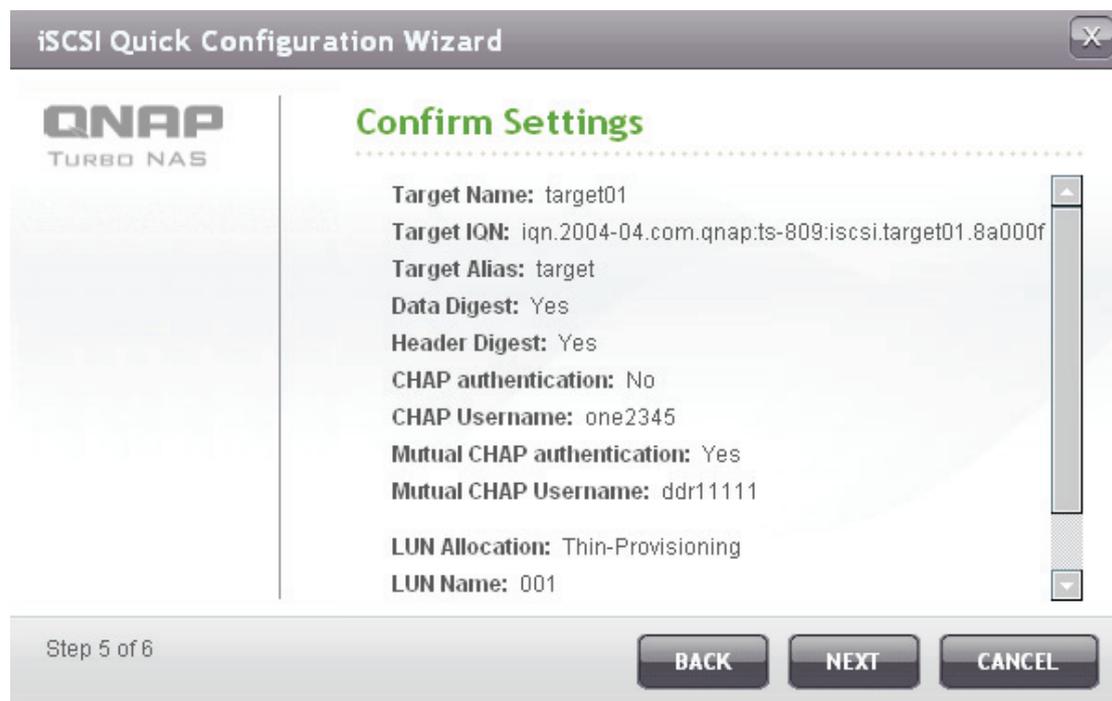
- Thin Provisioning: Select this option to allocate the disk space in a flexible manner. You can allocate the disk space to the target anytime regardless of the current storage capacity available on the NAS. Over-allocation is allowed since the storage capacity of the NAS can be expanded by online RAID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

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



The screenshot shows the 'iSCSI Quick Configuration Wizard' window. The title bar reads 'iSCSI Quick Configuration Wizard' with a close button. On the left is the 'QNAP TURBO NAS' logo. The main area is titled 'Create an iSCSI LUN'. It features two radio buttons for 'LUN Allocation': 'Thin-Provisioning' (selected) and 'Instant Allocation'. Below this are input fields for 'LUN Name' (containing '001'), 'LUN Location' (a dropdown menu showing '/share/HDB_DATA' and 'Free Size: 281.6GB'), and 'Capacity' (a slider set to '50' GB). At the bottom, it indicates 'Step 4 of 6' and has 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.

The screenshot displays the 'Target Management' section of a storage management interface. At the top, there is a 'QUICK CONFIGURATION WIZARD' button and a note: '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-809:iscsi.a.8a000f)	Ready	
	allen (iqn.2004-04.com.qnap:ts-809:iscsi.allen.8a000f)	Ready	
	david (iqn.2004-04.com.qnap:ts-809:iscsi.rrr.8a000f)	Ready	
	target (iqn.2004-04.com.qnap:ts-809:iscsi.target01.8a000f) └ id:0 - 001 (50.00 GB)	Ready Enabled	

Below the table, it says 'Total: 4 | Display 10 entries per page.' and includes navigation arrows. Underneath is the 'Un-Mapped iSCSI LUN List' table:

Name	Capacity	Action
22	1.00 GB	
52	281.68 GB	

At the bottom, it says 'Delete Total: 2 | Display 10 entries per page.' and includes navigation arrows.

Create more LUN for a target (Intel-based NAS models running firmware version 3.2.0 or later only)

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

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

The screenshot shows the 'iSCSI Configuration' page with three tabs: 'PORTAL MANAGEMENT', 'TARGET MANAGEMENT', and 'ADVANCED ACL'. The 'TARGET MANAGEMENT' tab is active. At the top, there is a 'QUICK CONFIGURATION WIZARD' button and a note: '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-809:iscsi.a.8a000f)	Ready	
	allen (iqn.2004-04.com.qnap:ts-809:iscsi.allen.8a000f)	Ready	
	david (iqn.2004-04.com.qnap:ts-809:iscsi.rrr.8a000f)	Ready	
	target (iqn.2004-04.com.qnap:ts-809:iscsi.target01.8a000f) └ id:0 - 001 (50.00 GB)	Ready Enabled	

Below the table, it says 'Total: 4 | Display 10 entries per page.' and includes navigation arrows.

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

Quick Configuration Wizard

QNAP
TURBO NAS

iSCSI Quick Configuration Wizard

I want to create

- iSCSI Target with a mapped LUN
- iSCSI Target only
- iSCSI LUN only

NEXT CANCEL

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

iSCSI Quick Configuration Wizard

QNAP
TURBO NAS

Create an iSCSI LUN

LUN Allocation: Thin-Provisioning Instant Allocation ⓘ

LUN Name: 002

LUN Location: /share/HDB_DATA Free Size: 281.6GB

Capacity: 1 GB

Step 1 of 4

NEXT CANCEL

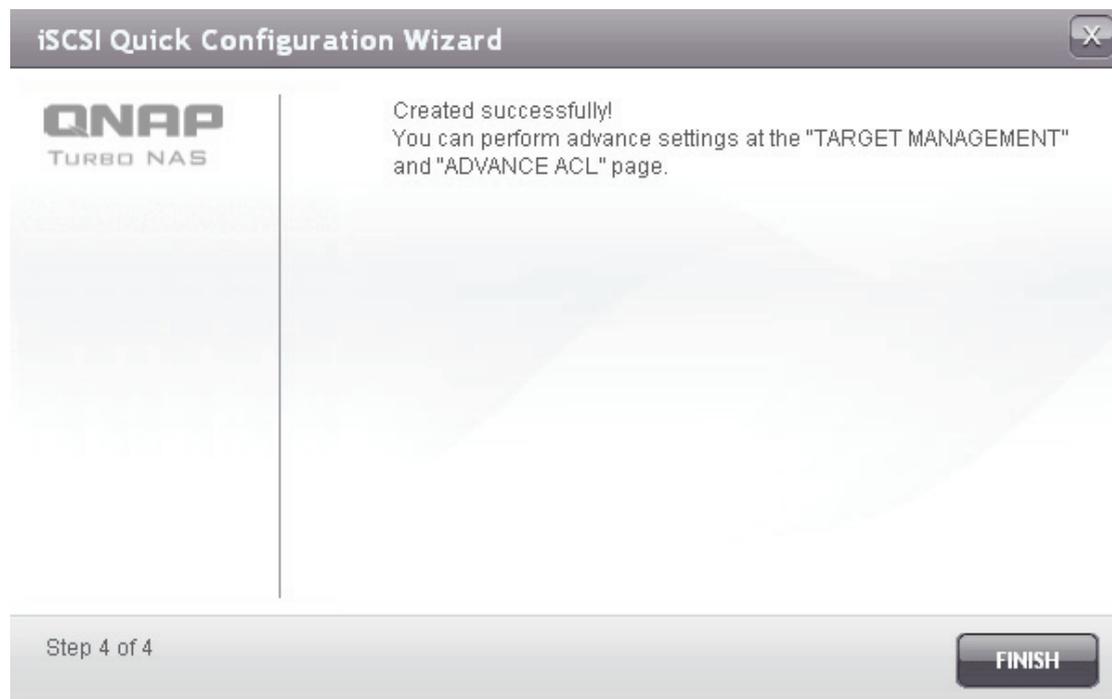
4. Select the target to map the LUN to. You can also select not to map the LUN for now.



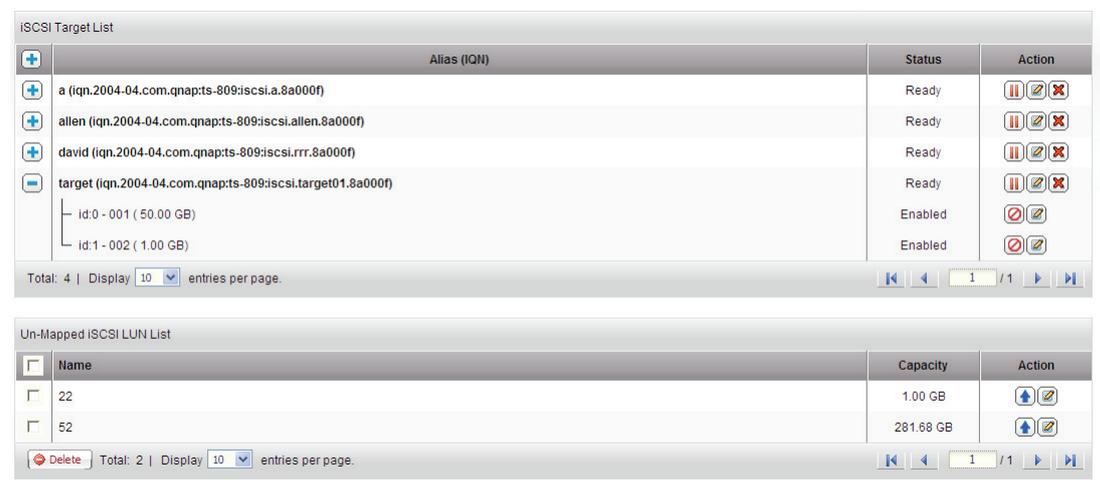
5. Confirm the settings and click 'Next'.



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



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



Item	Status	Description
iSCSI target	Ready	The iSCSI target is ready but no initiator has connected to it yet.
	Connected	The iSCSI target has been connected by an initiator.
	Disconnected	The iSCSI target has been disconnected.
	Offline	The iSCSI target has been inactive 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, and so on.
	Delete an iSCSI target. All the connections will be removed.
	Disable an LUN. All the connections will be removed.
	Enable an LUN.
	Unmap the LUN from the target. Note that you must disable the LUN first before unmapping the LUN. When you click this button, the LUN will be moved to 'Un-Mapped iSCSI LUN List'.
	Map the LUN to an iSCSI target. This option is only available on the 'Un-Mapped iSCSI LUN List'.
	View the connection status of an iSCSI target.

Switch the mapping of an LUN (Intel-based NAS models running firmware version 3.2.0 or later only)

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

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



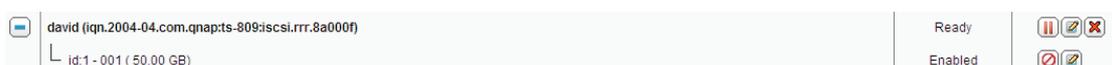
2. Next, click  (Unmap) to unmap the LUN. The LUN will appear on the Un-Mapped iSCSI LUN List. Click  (Map) to map the LUN to another target.

Un-Mapped iSCSI LUN List			
<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	001	50.00 GB	 

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



4. The LUN is mapped to the target.



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

Connect to the NAS using Microsoft iSCSI initiator in Windows

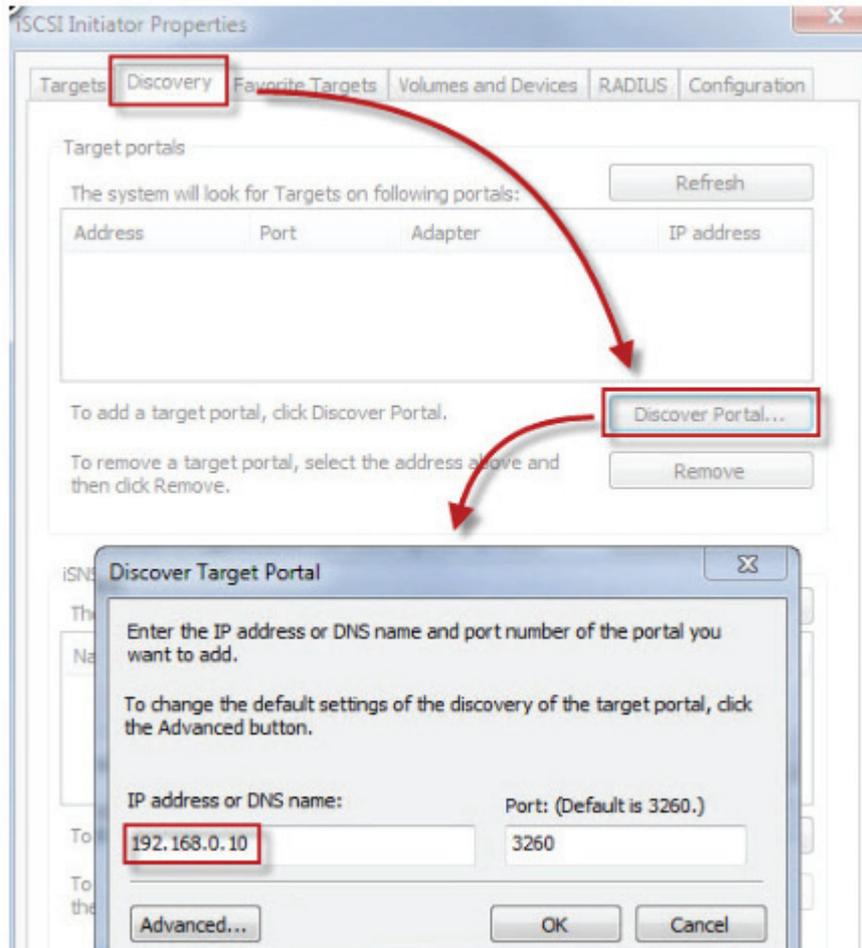
Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

iSCSI initiator on Windows

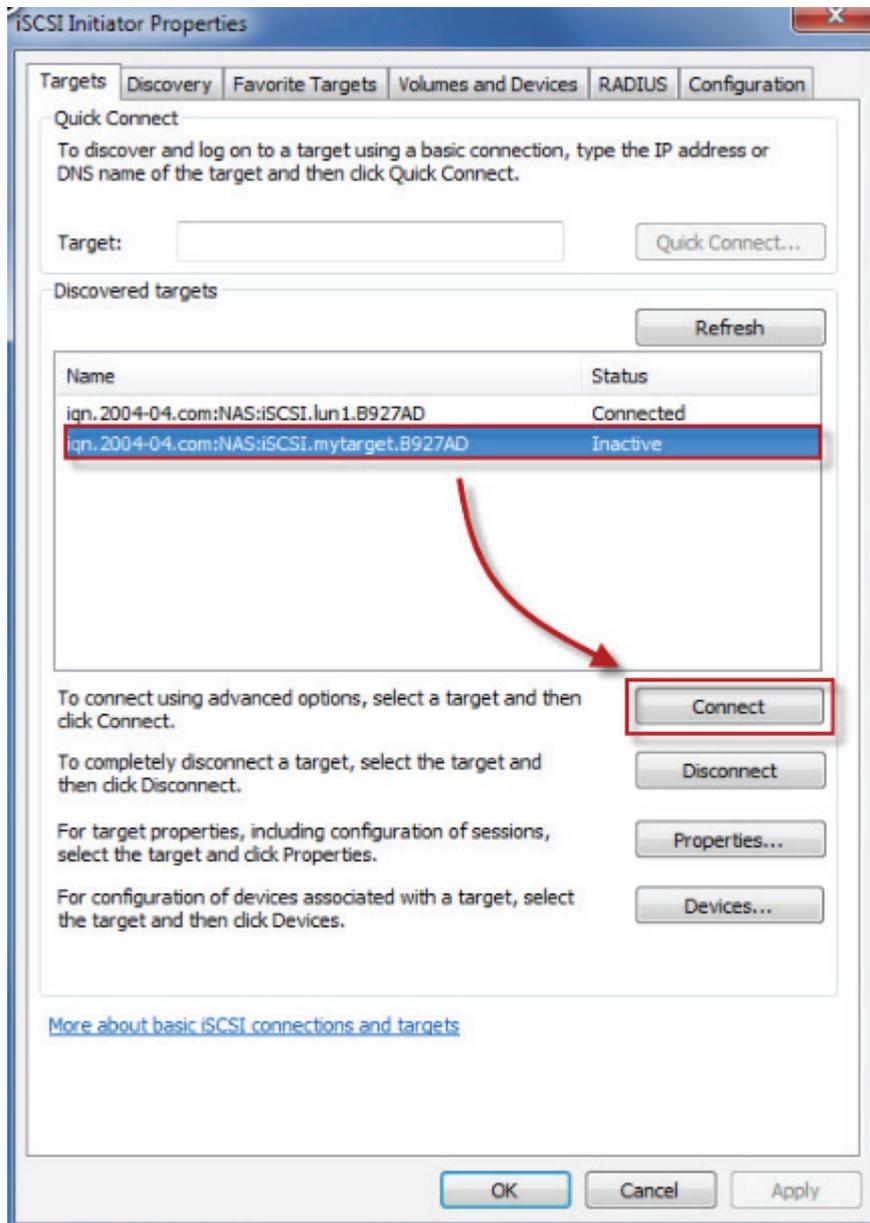
Microsoft iSCSI Software Initiator v2.07 is an official application for Windows OS 2003, XP, and 2000 to allow users to implement an external iSCSI storage array over the network. If you are using Windows Vista or Windows Server 2008, Microsoft iSCSI Software Initiator is included. For more information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

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

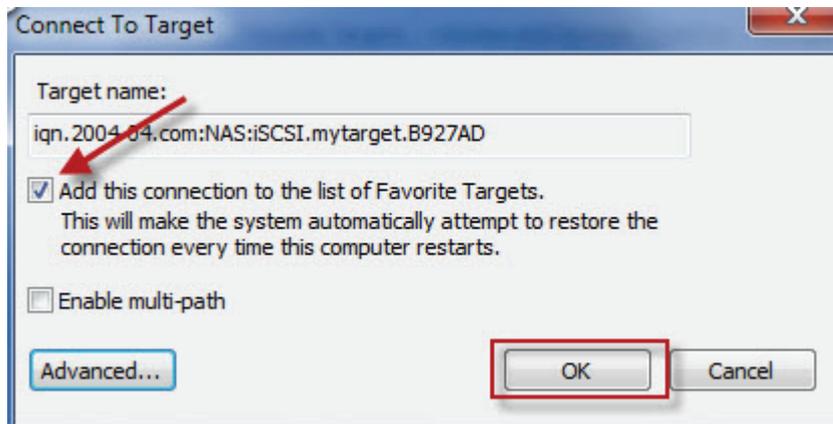
Start iSCSI initiator from 'Control Panel' > 'Administrative Tools'. Under the 'Discovery' tab click 'Add Portal'. Enter the NAS IP and the port number for the iSCSI service.



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'.



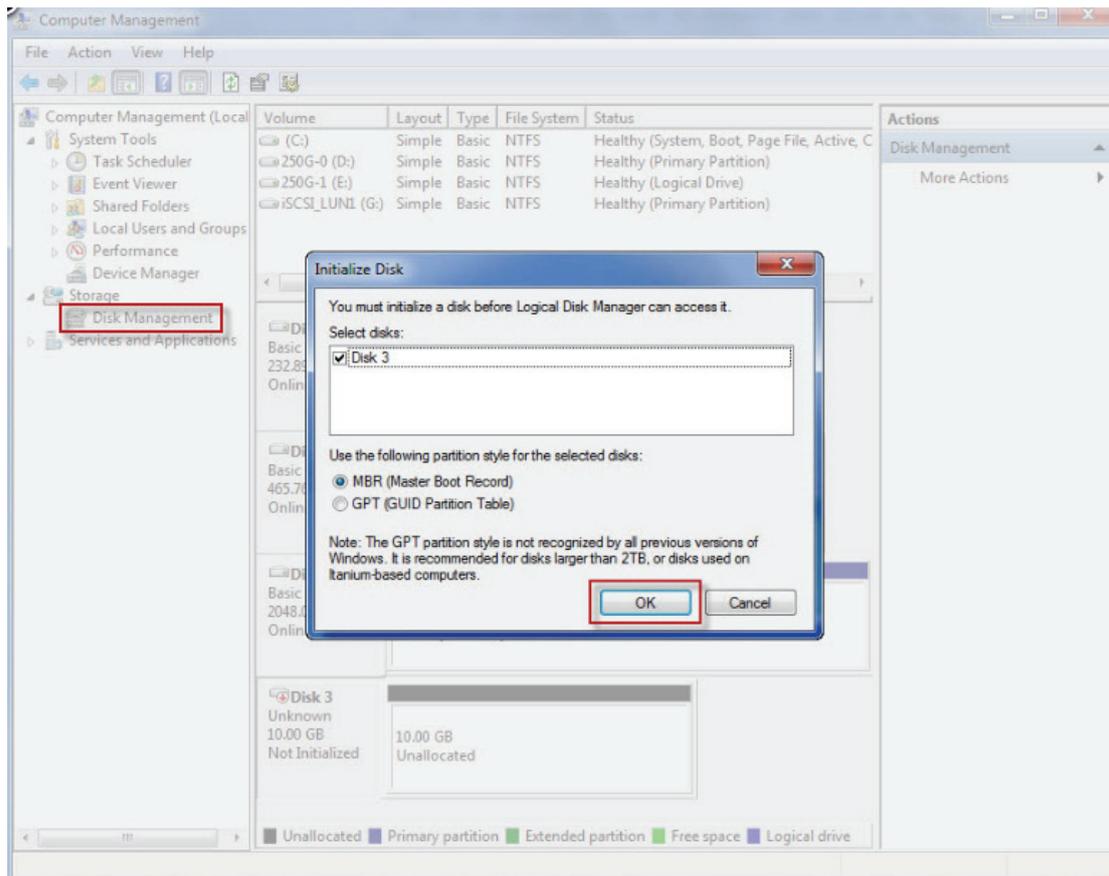
You may click 'Advanced' to specify the logon information if you have configured the authentication otherwise simply click 'OK' to continue.



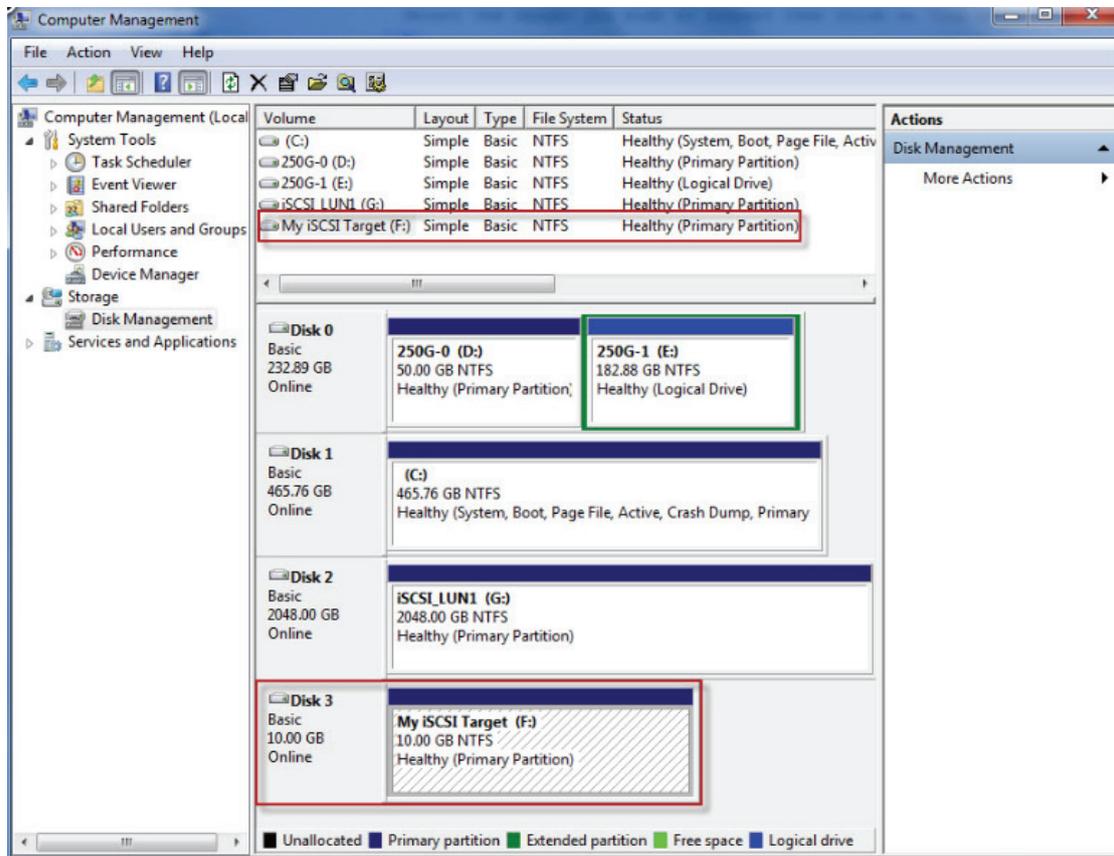
Upon successful logon, the status of the target now shows 'Connected'.

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 there was a new hard 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.



Connect to the NAS using globalSAN iSCSI initiator in Mac OS

This section shows you how to use globalSAN 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 globalSAN iSCSI initiator

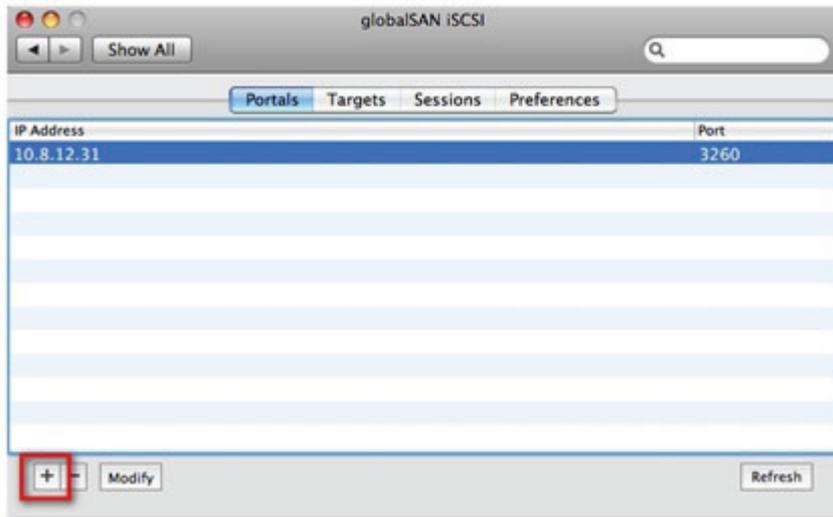
globalSAN initiator (3.3.0.43) is a Universal Application, for Intel- and PowerPC-based Mac computers (system requirements: Mac OS X 10.4 or later). It provides a user-friendly interface which allows the users to easily connect to an iSCSI volume. For more information & download location, visit:

http://www.studionetworksolutions.com/products/product_detail.php?t=moren=1
1

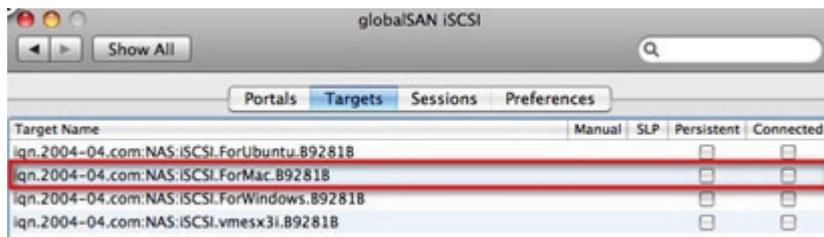
Run the iSCSI initiator in 'System Preference'.



Click '+'. Enter the NAS IP to add a new portal.



The available iSCSI targets will be shown in 'Targets' automatically. Check the 'Connected' box of the iSCSI target that you want to connect.



Enter the login information to connect to the iSCSI target.

The screenshot shows the iSCSI configuration dialog box for the target `iqn.2004-04.com:NAS:iSCSI.ForMac.B9281B`. The **General** tab is selected. Under the **CRC / Checksum** section, both **Data Digest** and **Header Digest** are unchecked. The **Connections** table lists one entry:

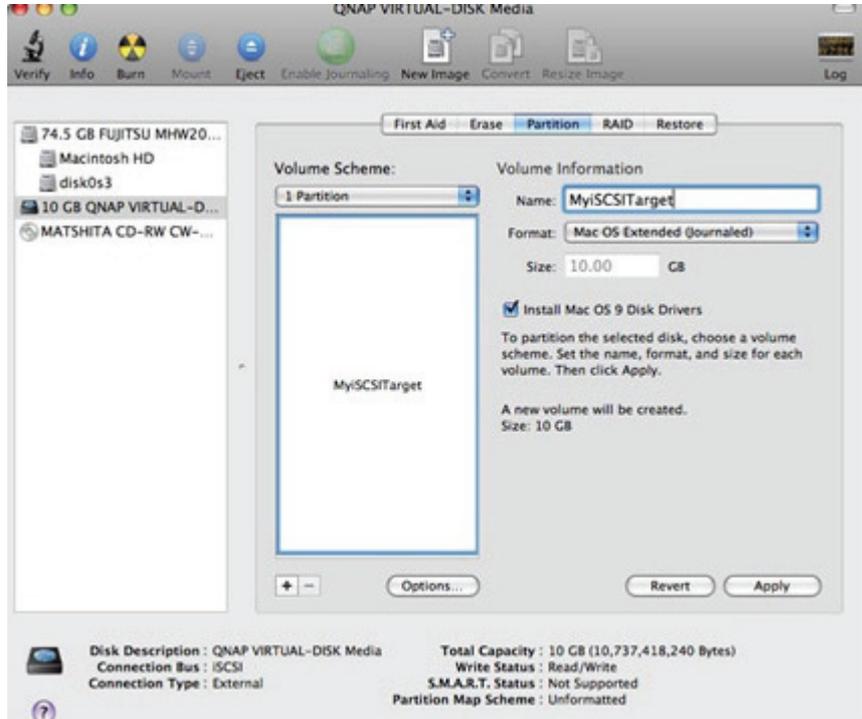
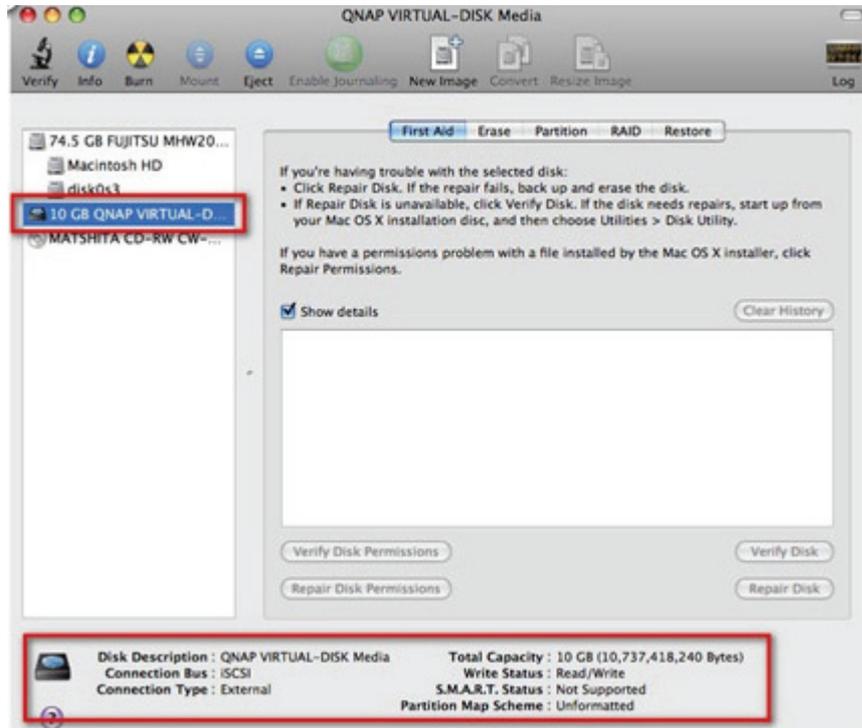
Target Address	Port
10.8.12.31	3260

Below the table, a note states: "For multiple target addresses to be effective, distinct routes to them must be configured in the Network panel of System Preferences". The **CHAP** tab is selected, and **Use CHAP Login Information** is checked. The **User Name** is `james`, the **Target Secret** is masked with dots, and the **Initiator Secret** field is empty. The **Make this target connection persistent** checkbox is unchecked. **Connect** and **Cancel** buttons are at the bottom.

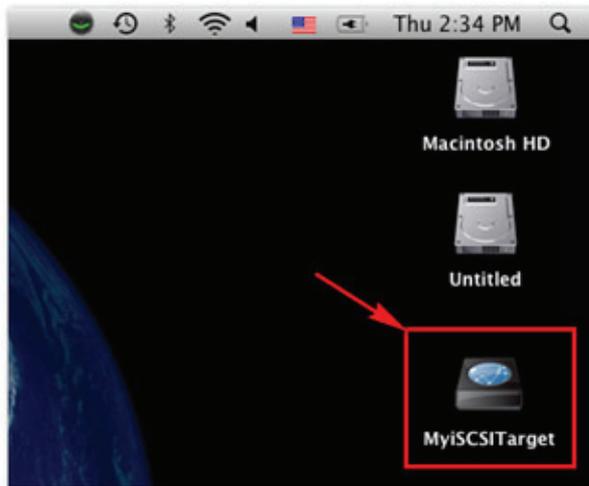
The first time you logon to the iSCSI target, a popup message will be shown to remind you the disk is not initialized. Click 'Initialize...' to format the disk. You can also open the 'Disk Utilities' application to do the initialization.



Format the iSCSI target.



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



Connect to the NAS using Open-iSCSI Initiator in 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 don't 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:

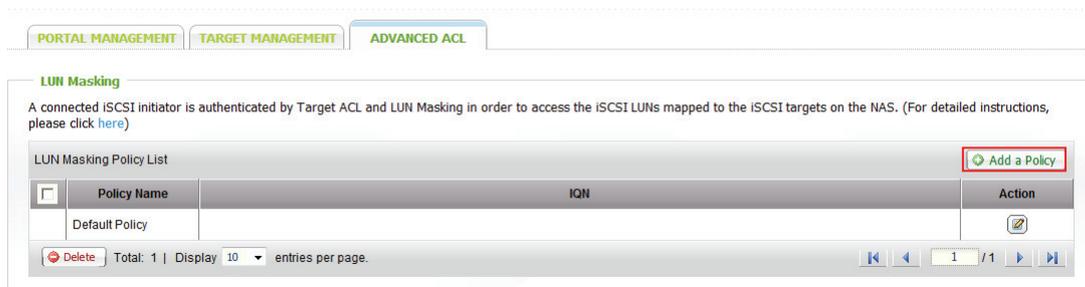
```
# iscsiadm -m node --op delete --targetname THE_TARGET_IQN
```

3.2.5.2 **ADVANCED ACL**

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

Intel-based NAS refers to TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, and TS-809U-RP

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



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

- Read-only: The connected initiator can only read the data from the LUN.
- Read/Write: The connected initiator has read and write access 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"/>	<div style="border: 1px solid #ccc; height: 100%; width: 100%; position: relative;"> <div style="position: absolute; top: -10px; right: -10px;">▲</div> <div style="position: absolute; bottom: -10px; right: -10px;">▼</div> </div>
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](#))

➕ Add a Policy

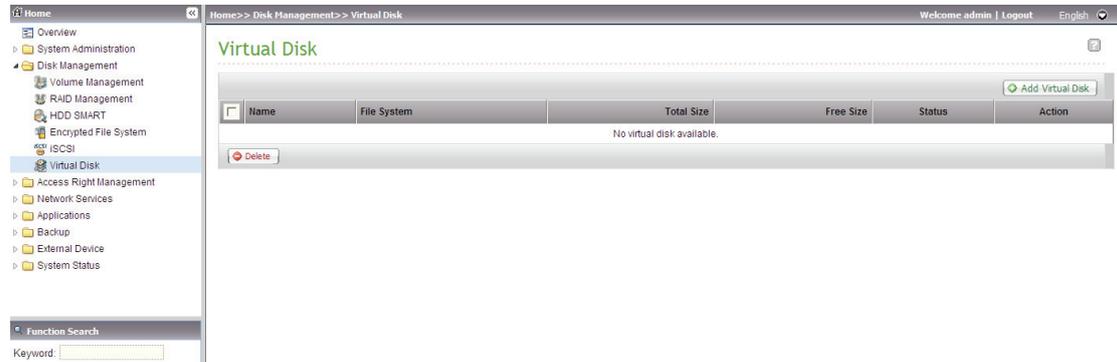
LUN Masking Policy List

☐	Policy Name	IQN	Action
☐	Default Policy		

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

3.2.6 Virtual Disk

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



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



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

Add Virtual Disk

Target Server IP: 10 . 8 . 10 . 39 Port : 3260

GET REMOTE DISK

Remote Disk Device: iqn.2004-04.com.qnap:SS-839;iSCSI.test.AABB1A

Authentication

User Name:

Password:

APPLY CANCEL

Click  to format the virtual disk.

<input type="checkbox"/>	Name	File System	Total Size	Free Size	Status	Action
<input type="checkbox"/>	VirtualDisk1	Unknown	5 GB	0 MB	Unmounted	  

Delete

When the status of the virtual disk is 'Ready', you can start to use the virtual disk as a disk volume of the NAS.

3.3 Access Right Management

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



3.3.1 Users

The NAS has created the following users by default:

- **admin**
By default, the administrator 'admin' has access right to the system administration and cannot be deleted.
- **guest**
This is a built-in user and will not be displayed on the 'User Management' page. A guest does not belong to any user group. The login password 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.

See the table below for more details:

Maximum number of users	NAS models
1,024	TS-110, TS-210
2,048	TS-119, TS-219, TS-219P, TS-410
4,096	TS-419P, TS-410U, TS-419U, TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, TS-809U-RP

The following information is required to create a new user:

✓ **User name**

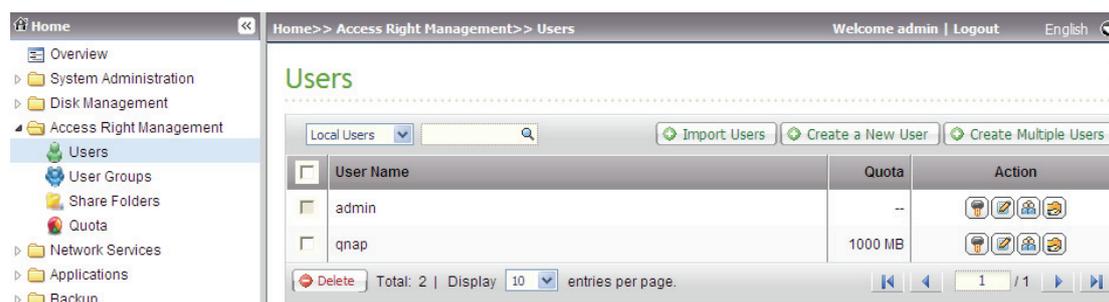
The user name must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean.

The invalid characters are listed below:

“ / \ [] : ; | = , + * ? < > ` ` `

✓ **Password**

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

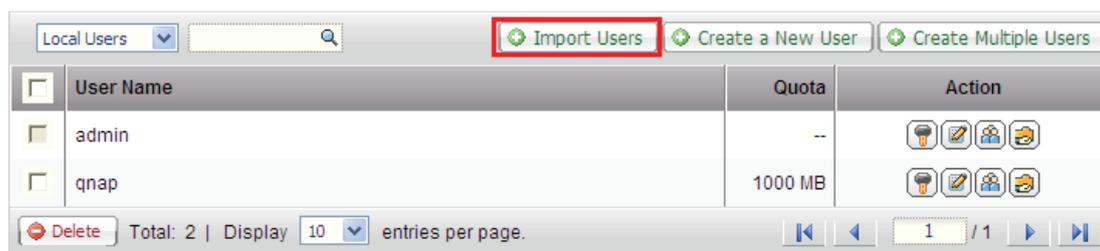


Import Users

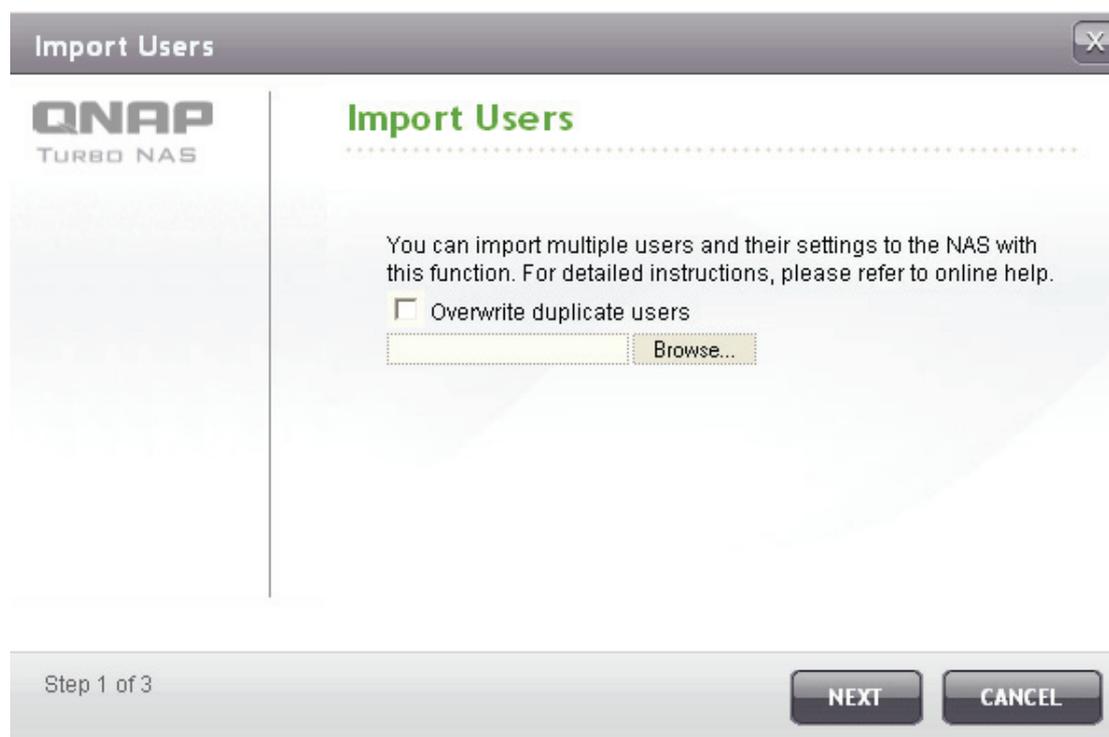
You can import multiple user accounts to the NAS with this feature. To import multiple users, follow the steps below:

1. Click 'Import Users'.

Users



2. Select the option 'Overwrite duplicate users' if you want to replace the existing users.
3. Select the file of users and click 'Next'.



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

Import Users
✕

Import User Preview

User Name	Password	Quota	Group Name	Status
test	test	2000	test	--
user01	user01	2000	test	--
user02	user02	2000	test	--
user03	user03	No limit	test	--
user04	user04	2000	test	--
user05	user05	2000	test	--
--	user06	2000	test	Please enter User Name.
user07	user07	2000	test	--

Step 2 of 3

BACK

NEXT

CANCEL

- The imported user accounts will be shown.

Users
?

Local Users
🔍

[Import Users](#)
[Create a New User](#)
[Create Multiple Users](#)

<input type="checkbox"/>	User Name	Quota	Action
<input type="checkbox"/>	admin	--	
<input type="checkbox"/>	test	--	
<input type="checkbox"/>	user01	--	
<input type="checkbox"/>	user02	--	
<input type="checkbox"/>	user03	--	
<input type="checkbox"/>	user04	--	
<input type="checkbox"/>	user05	--	
<input type="checkbox"/>	user07	--	

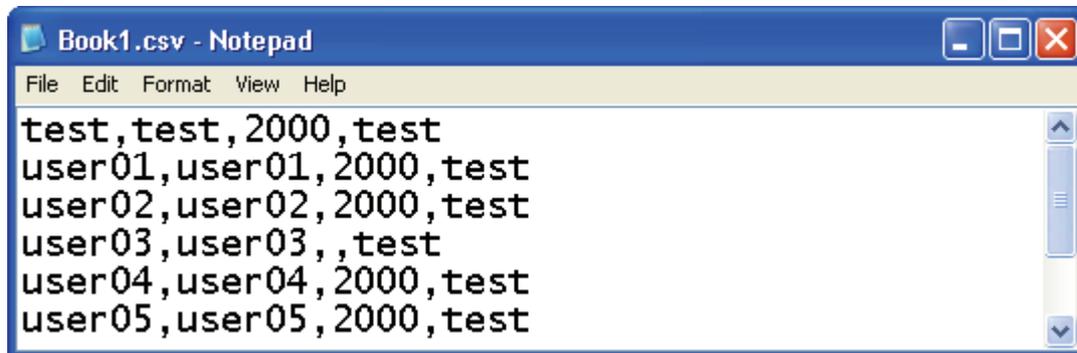
Delete
Total: 8 | Display 10 entries per page.
⏪ ⏩ 1 / 1 ⏪ ⏩

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

txt

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

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



```
test,test,2000,test
user01,user01,2000,test
user02,user02,2000,test
user03,user03,,test
user04,user04,2000,test
user05,user05,2000,test
```

csv (Excel)

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

An example is shown as below:

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

3.3.2 User Groups

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:

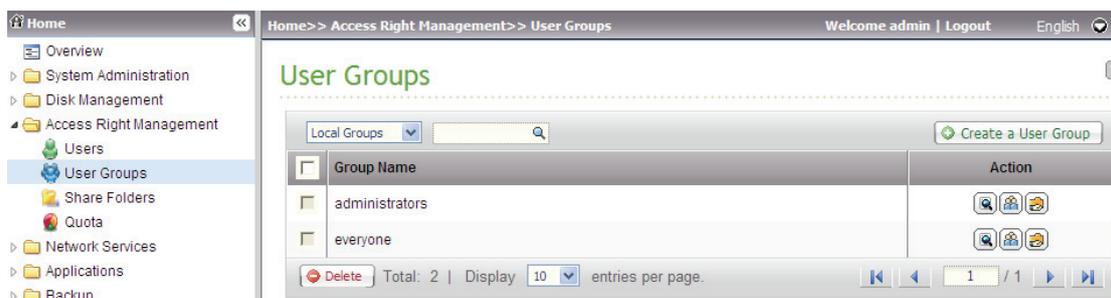
- **administrators**
All the members in this group have the administration right of the NAS. You cannot delete this group.
- **everyone**
All the registered users belong to everyone group. You cannot delete this group.

The number of user groups you can create on the NAS varies according to the NAS models. See the table below for more details:

Maximum number of user groups	NAS models
128	TS-110, TS-210
256	TS-119, TS-219, TS-219P, TS-410
512	TS-419P, TS-410U, TS-419U, TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, TS-809U-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:

“ / \ [] : ; | = , + * ? < > ` `



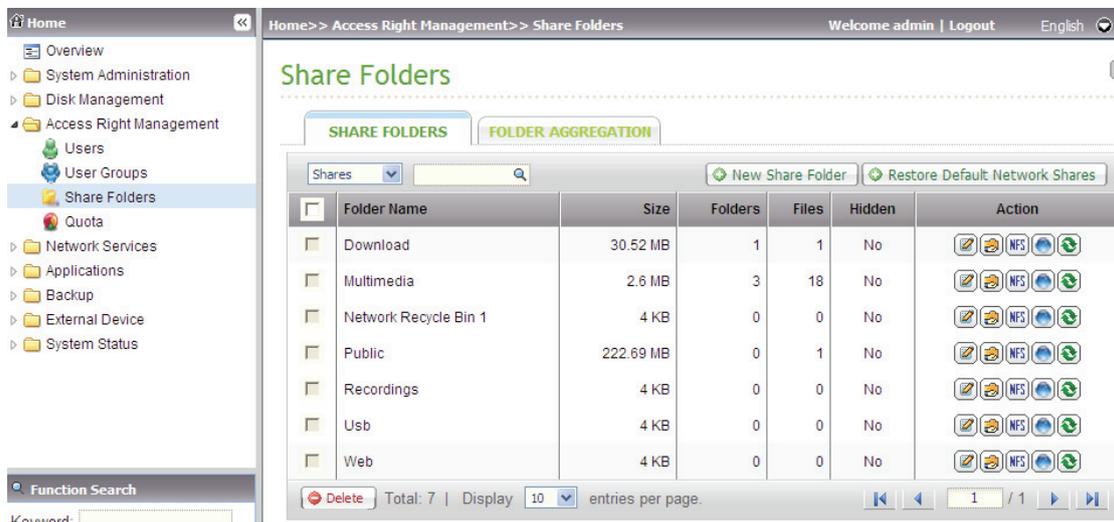
3.3.3 Share Folders

3.3.3.1 Share Folder

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

The number of share folders you can create on the NAS varies according to the NAS models. See the table below for more details:

Maximum number of share folders	NAS models
256	TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410
512	TS-419P, TS-410U, TS-419U, TS-239 Pro, TS-239 Pro II, TS-259 Pro, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, TS-809U-RP



3.3.3.2 Folder Aggregation

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

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 page with the 'Folder Aggregation' tab selected. The 'Folder Aggregation' section is expanded, showing a checked checkbox for 'Enable Folder Aggregation'. 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.' An 'APPLY' button is located at the bottom right of this section. Below the 'Folder Aggregation' section is the 'Folder Aggregation List' section, which contains 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'. A 'Delete' button is located below the table.

2. Click 'Create A Portal Folder'.

This screenshot shows the 'Folder Aggregation List' section. The 'Create A Portal Folder' button is highlighted with a red rectangle. The table below it has two columns: 'Portal Folder Name' and 'Action'. A 'Delete' button is located below the table.

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

Step 1 of 1

APPLY CANCEL

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

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

Folder Aggregation List

Create A Portal Folder Import/ Export Folder Tree

Portal Folder Name	Action
shares	 

Delete

Remote Folder Link
✕

Remote Folder Link

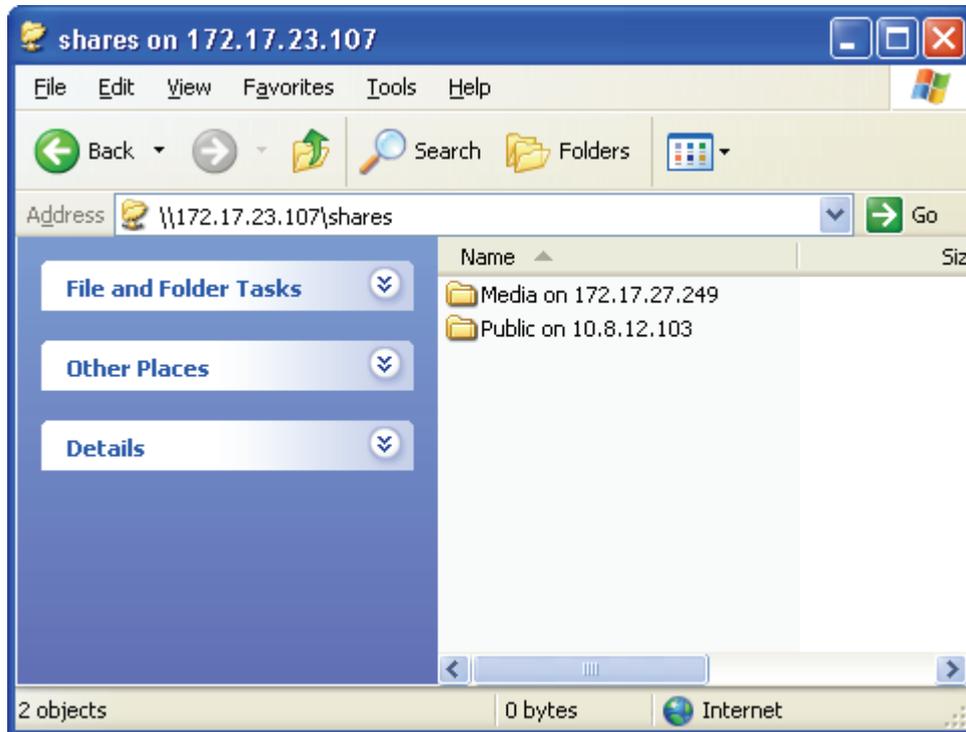
Portal Folder Name: Shares

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

Step 1 of 1

APPLY
CANCEL

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



3.3.4 Quota

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

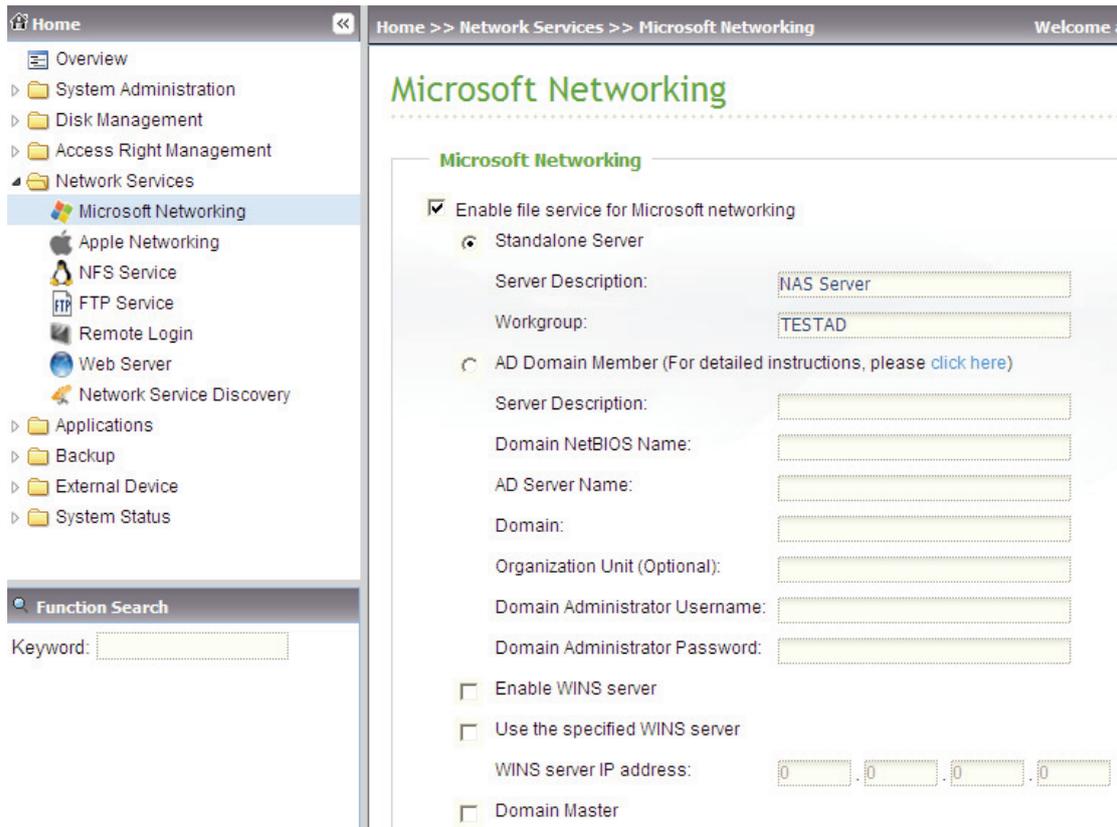
- ✓ Enable quota for all users
- ✓ Quota size on each disk volume



3.4 Network Services



3.4.1 Microsoft Networking



Enable file service for Microsoft networking: If you are using Microsoft Windows, turn on this option so that you can access the files on the network share folders. Assign a workgroup name.

✓ **Standalone Server**

Use local users for user authentication.

✓ **AD Domain Member**

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

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

➤ **Server Description**

Describe the NAS for the users to identify the server. To use the NAS on the Microsoft Windows OS, you must enable Microsoft Network Services.

➤ **Workgroup**

Specify the workgroup the NAS belongs to. The workgroup is a computer group unit on Microsoft Windows network for network sharing.

➤ **AD Server Name**

Enter the name of the AD server when the AD domain is selected for authentication.

➤ **Domain Name**

The name of the Microsoft domain. When you select AD domain, you must enter the domain name, the login user name, and the password.

For the information of joining the NAS to Active Directory, see [Chapter 8](#).

✓ **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.

✓ **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.

3.4.2 Apple Networking

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



3.4.3 NFS Service

To access the NAS from Linux, enable the NFS service.

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 folder 'public' under the /mnt/pub directory, use the following command:

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

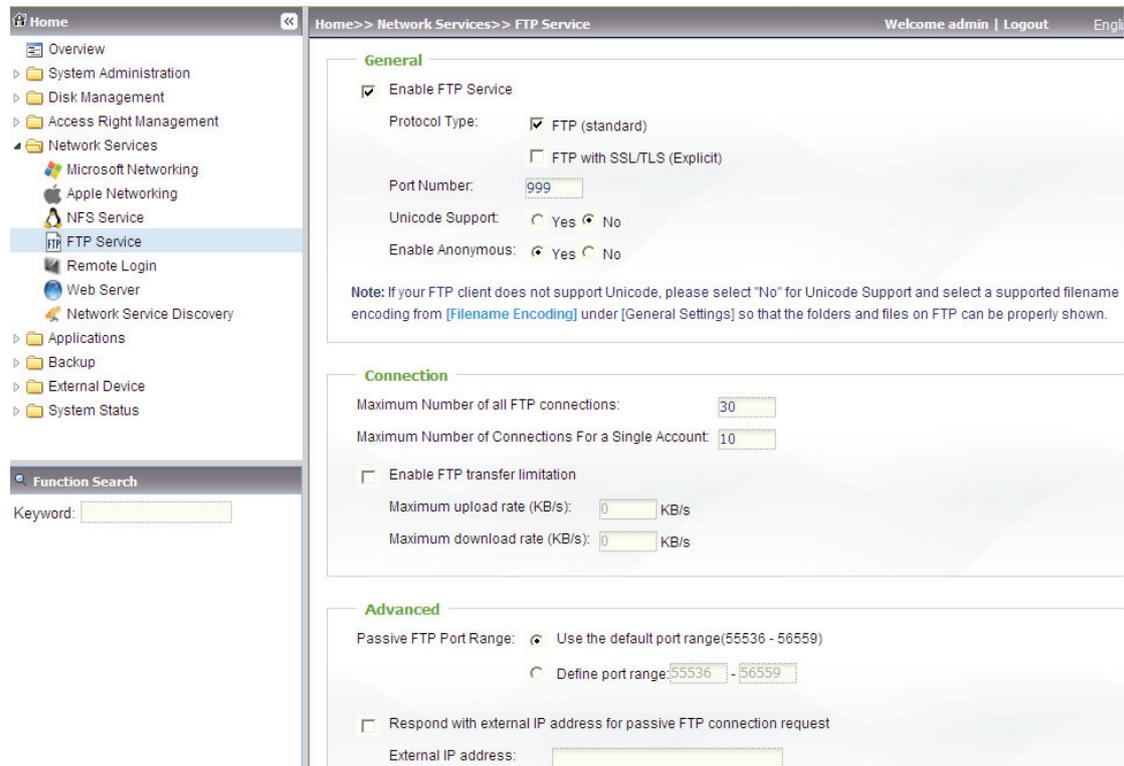
Note: You must login as the 'root' user to initiate the above command.

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



3.4.4 FTP Service

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



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

✓ **Select 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.

'SFTP' requires SSH to be enabled. Only the 'admin' user account can connect to the NAS by SFTP.

✓ **Unicode Support**

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

✓ **Anonymous Login**

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

✓ **Passive FTP Port Range**

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

✓ **FTP Transfer Limitation**

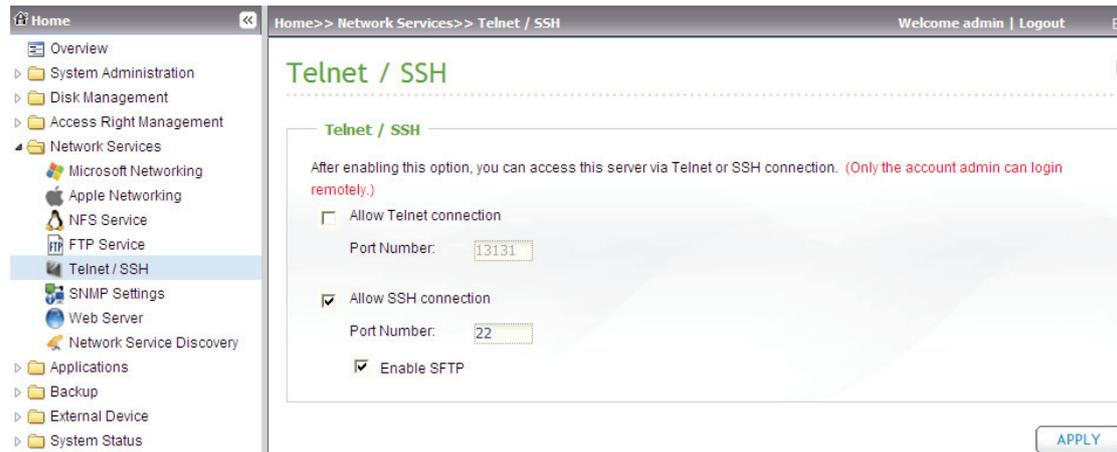
Specify the maximum number of FTP connections, maximum connections of a single user account and the maximum upload/ download rates of a single connection.

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

When passive FTP connection is in use, the FTP server (NAS) is behind a router, and a remote computer cannot connect to the FTP server over the WAN, enable this function. When this option is turned on, the NAS replies the IP address you specify or automatically detects the external IP address so that the remote computer is able to connect to the FTP server.

3.4.5 Telnet/SSH

You can turn on this option to connect to the NAS by Telnet or SSH encrypted connection (only the 'admin' account can login remotely). You can use Telnet or SSH connection clients, for example, putty for connection. Make sure you have opened the ports you specified on your router or firewall.



3.4.6 SNMP Settings

You can enable SNMP (Simple Network Management Protocol) service on the NAS and enter the trap address of the SNMP management stations (SNMP manager), 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. You can 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. You can specify the authentication and privacy settings if available.

Home >> Network Services >> SNMP Settings

Welcome admin | Logout

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 [\[Download\]](#).

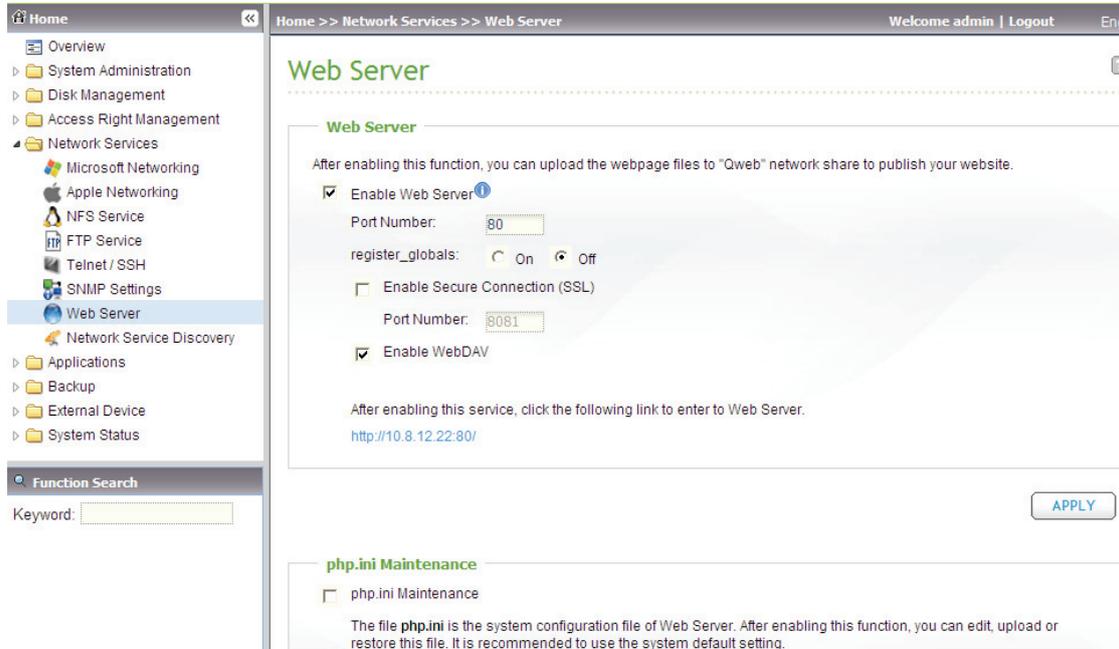
[DOWNLOAD](#)

Function Search
Keyword:

- Overview
- System Administration
- Disk Management
- Access Right Management
- Network Services
 - Microsoft Networking
 - Apple Networking
 - NFS Service
 - FTP Service
 - Telnet / SSH
 - SNMP Settings**
 - Web Server
 - Network Service Discovery
- Applications
- Backup
- External Device
- System Status

3.4.7 Web Server

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



To use Web Server, follow the steps below.

1. Enable the service and enter the port number. The default number is 80.
2. Configure other settings:
 - **Configure register_globals**

Select to enable or disable register_globals. The setting is disabled by default. When the web program 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)**

Specify the port number for SSL connection.

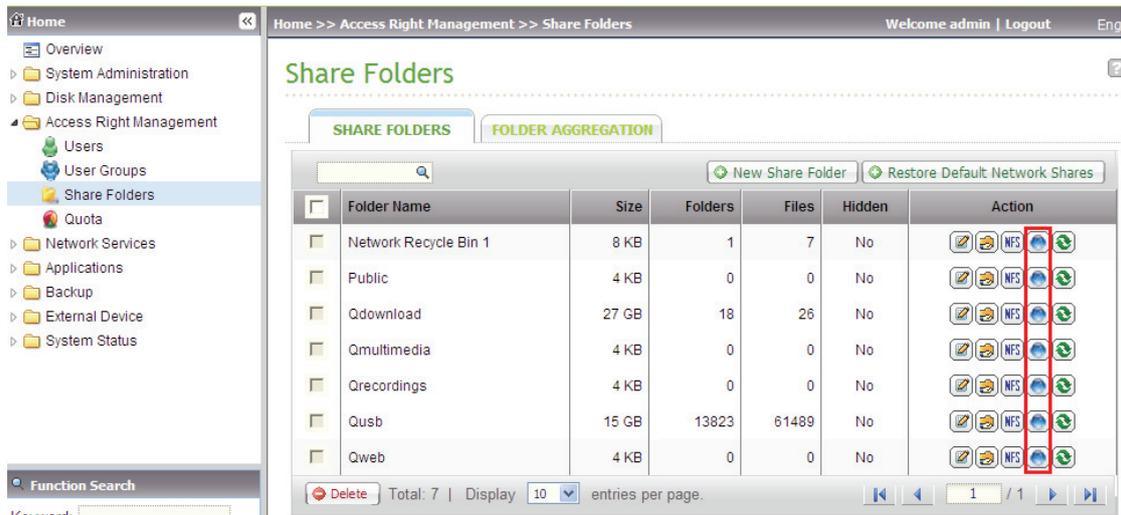
3. Upload the HTML files to the share folder (Qweb/ Web) on the NAS. The file index.html, index.htm or index.php will be the home path of your web page.
4. You can connect to the web page by entering http://NAS IP/ in the web browser. Note that when Web Server is enabled, you have to enter http://NAS IP:8080 in your web browser to connect to the login page of the NAS.

3.4.7.1 WebDAV

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

To map a share folder 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 share folders.

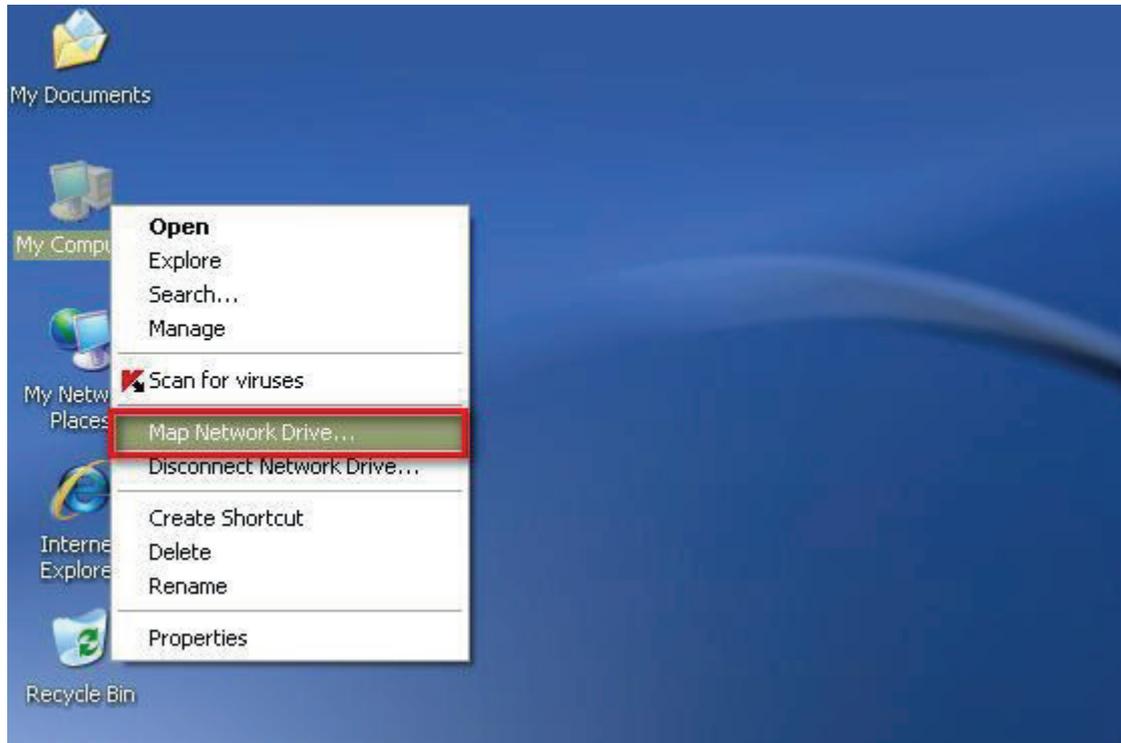


Folder Name	Size	Folders	Files	Hidden	Action
Network Recycle Bin 1	8 KB	1	7	No	
Public	4 KB	0	0	No	
Qdownload	27 GB	18	26	No	
Qmultimedia	4 KB	0	0	No	
Qrecordings	4 KB	0	0	No	
Qusb	15 GB	13823	61489	No	
Qweb	4 KB	0	0	No	

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

Windows XP:

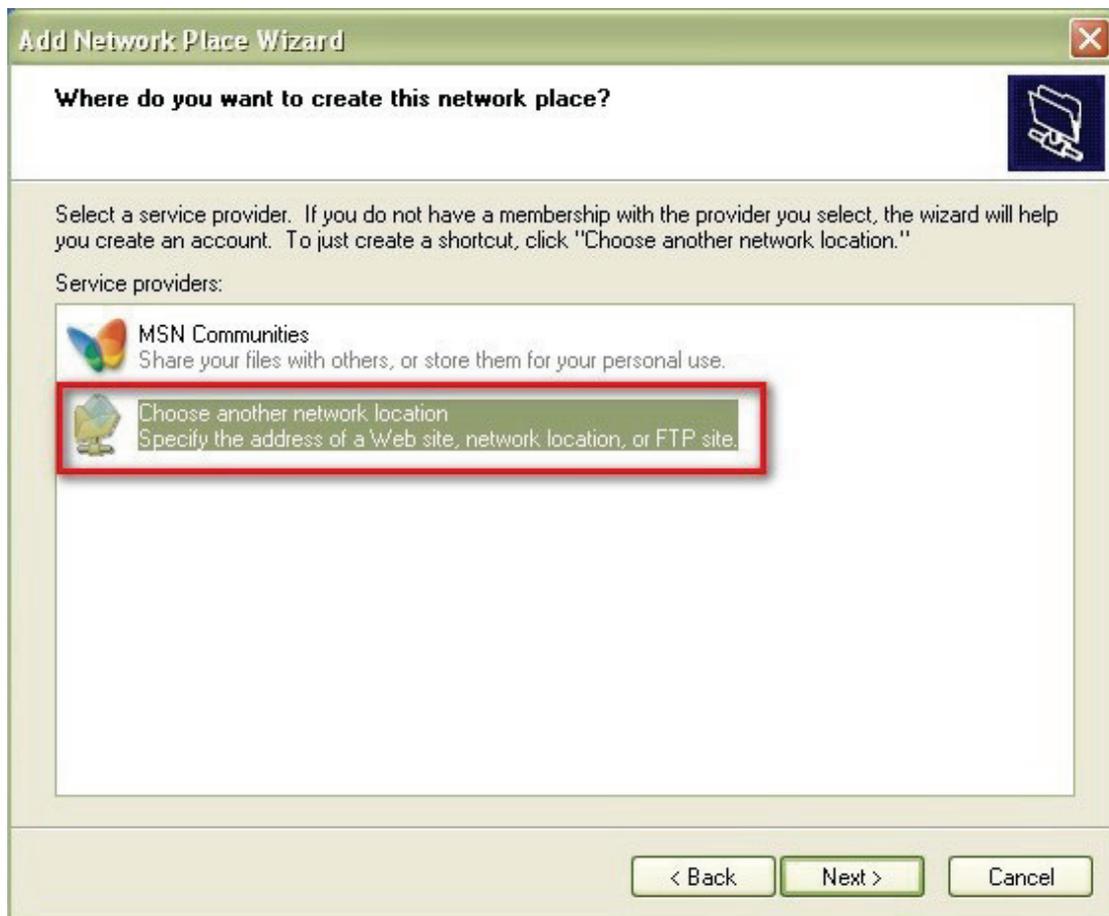
1. Right click 'My Computer' and select 'Map Network Drive...'



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

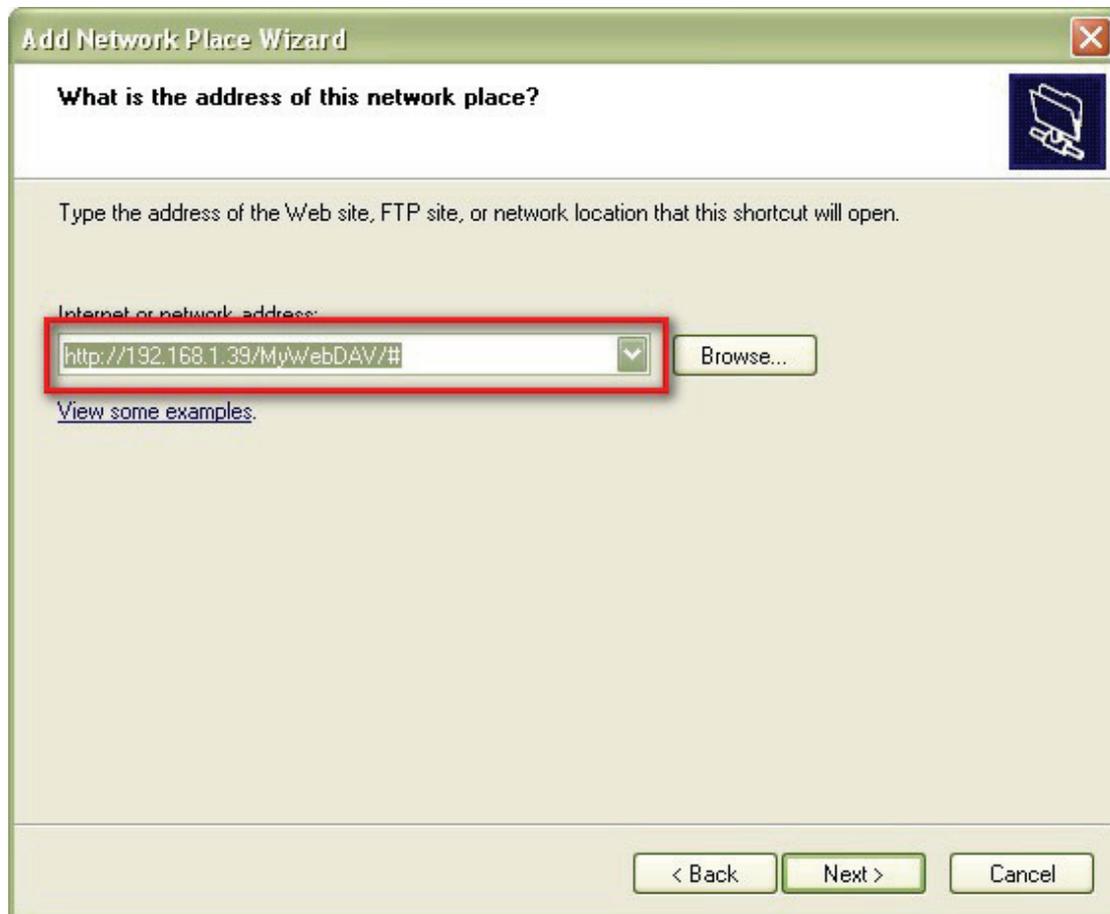


3. Select 'Choose another network location'.



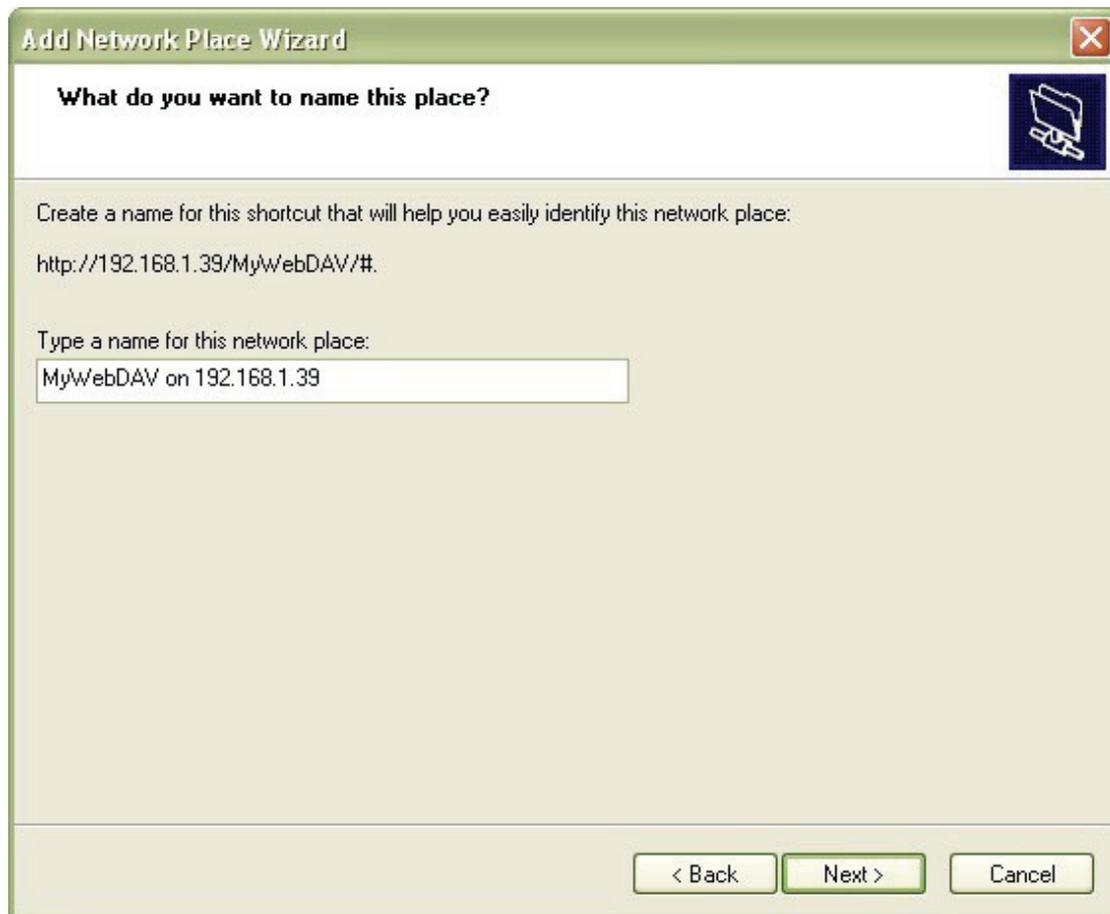
4. Enter the URL of your NAS with the share folder name. Note that you should put a '#' key at the end of the URL. Click 'Next'.

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



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

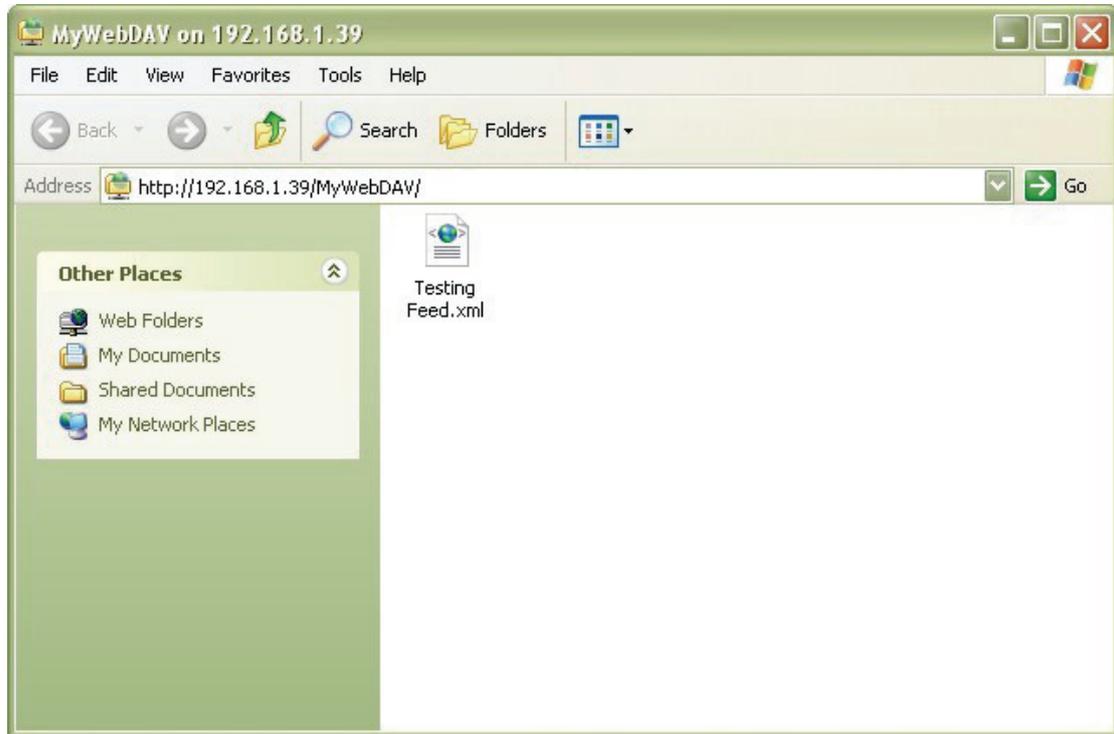
6. Type a name for this network place.



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



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

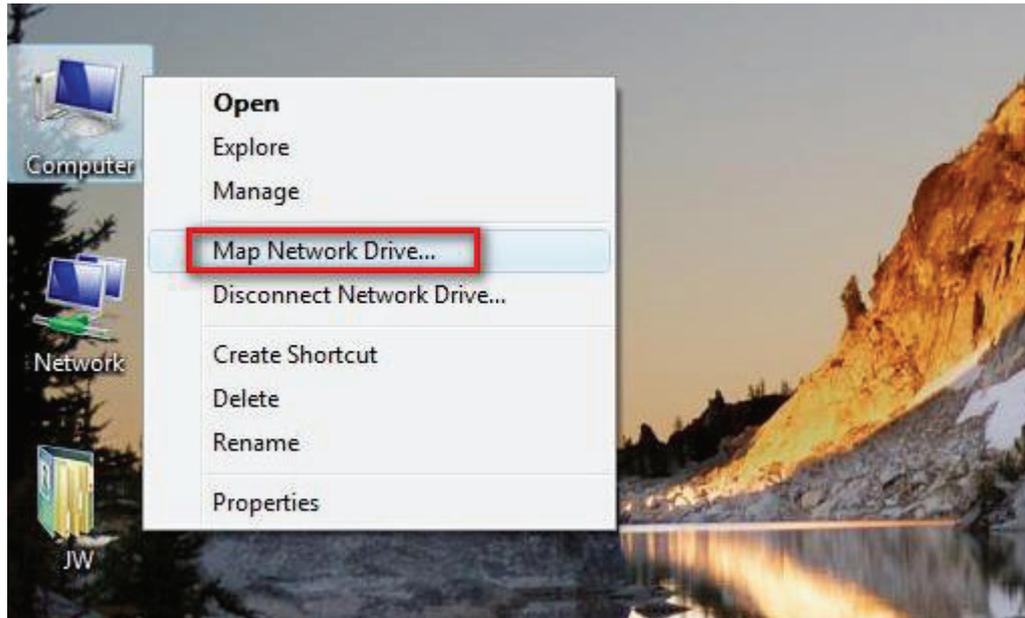


Windows Vista

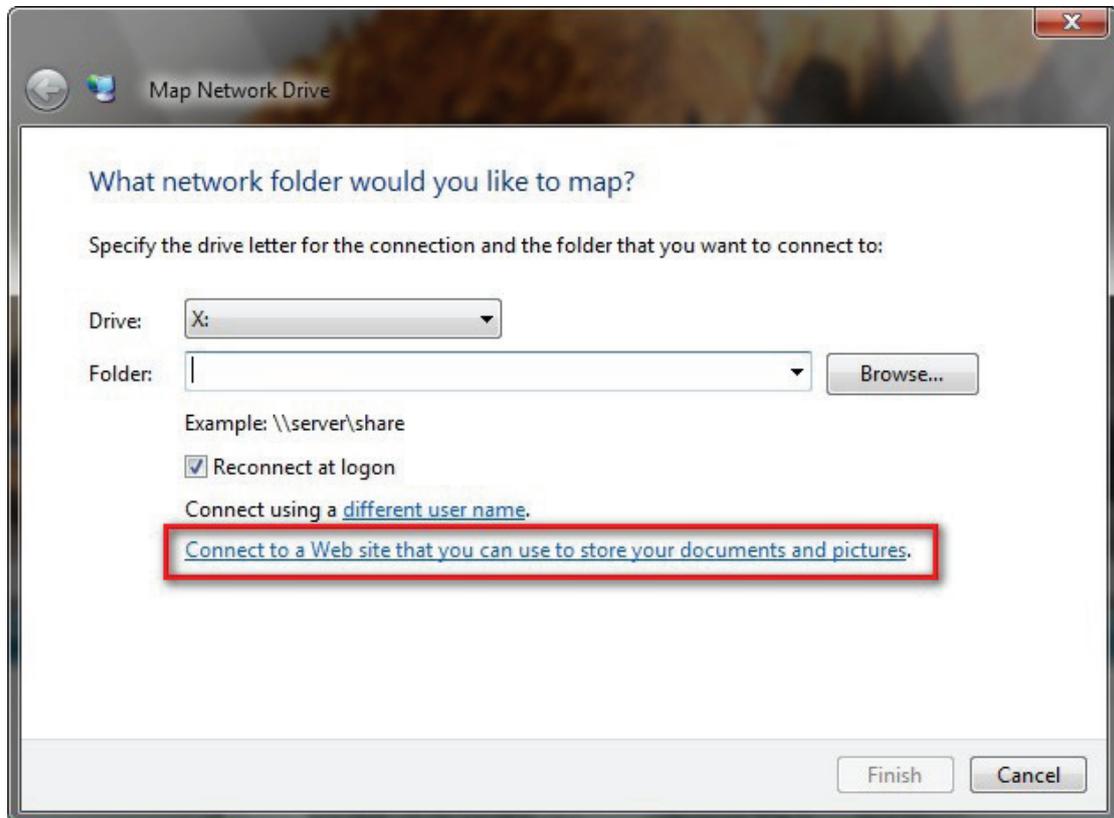
If you are using Windows Vista, you might need to install the 'Software Update for Web Folders (KB907306)'. This update is for 32-bit Windows OS only.

<http://www.microsoft.com/downloads/details.aspx?FamilyId=17c36612-632e-4c04-9382-987622ed1d64&displaylang=en>

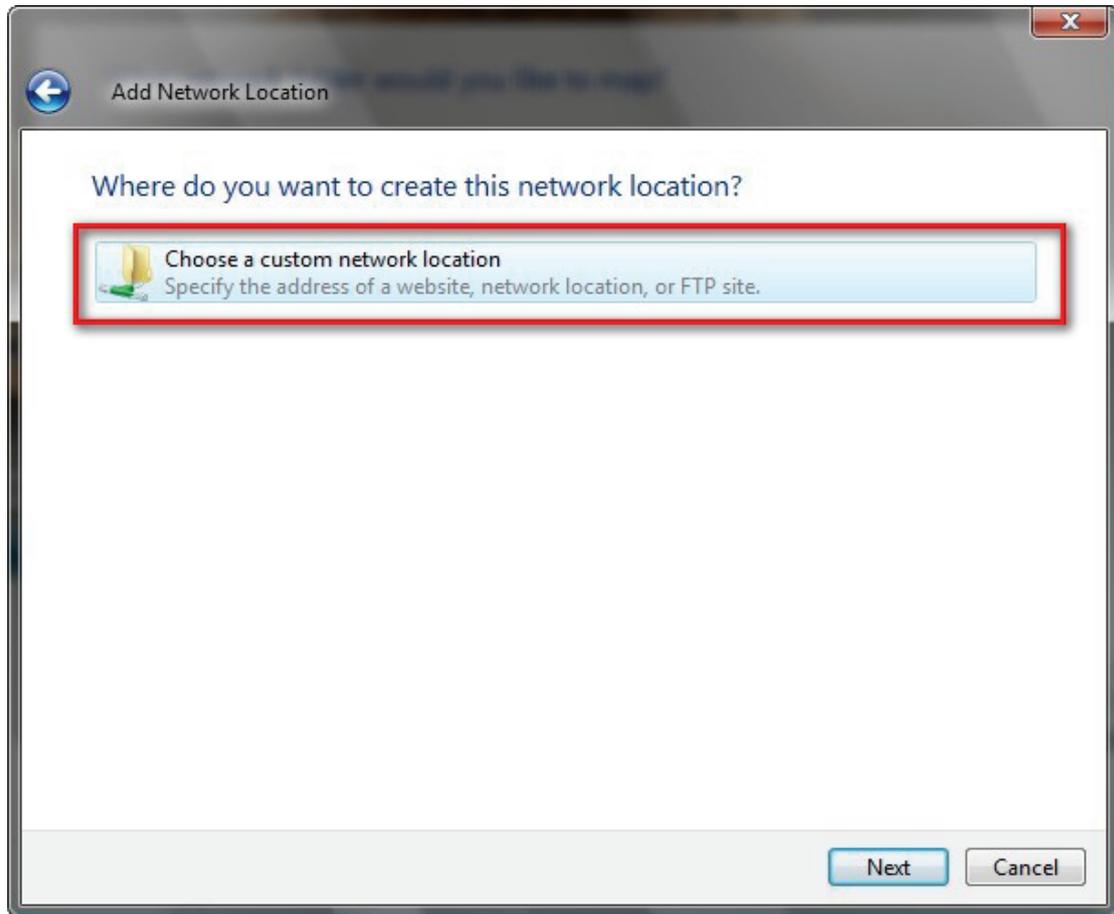
1. Right click 'Computer' and select 'Map Network Drive...'



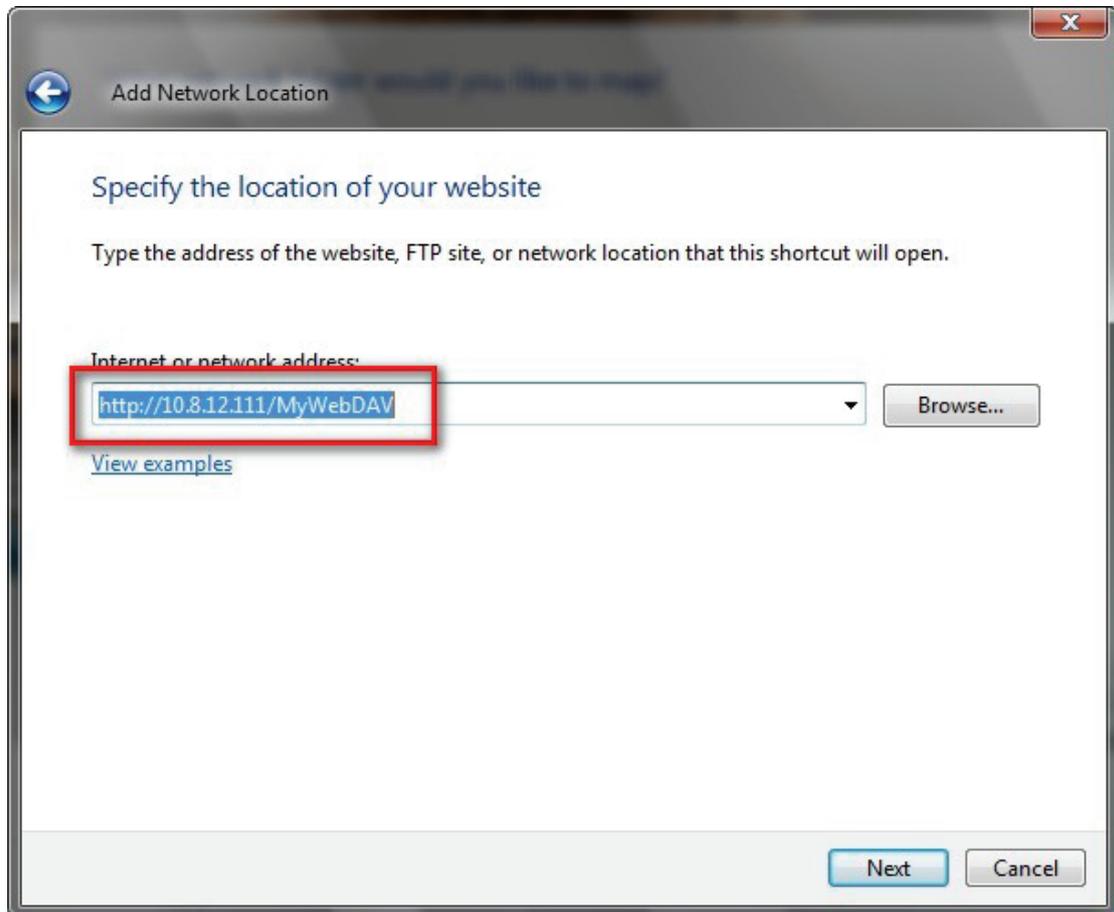
2. Click 'Connect to a Web site that you can use to store your documents and pictures'.



3. Select 'Choose a custom network location'.

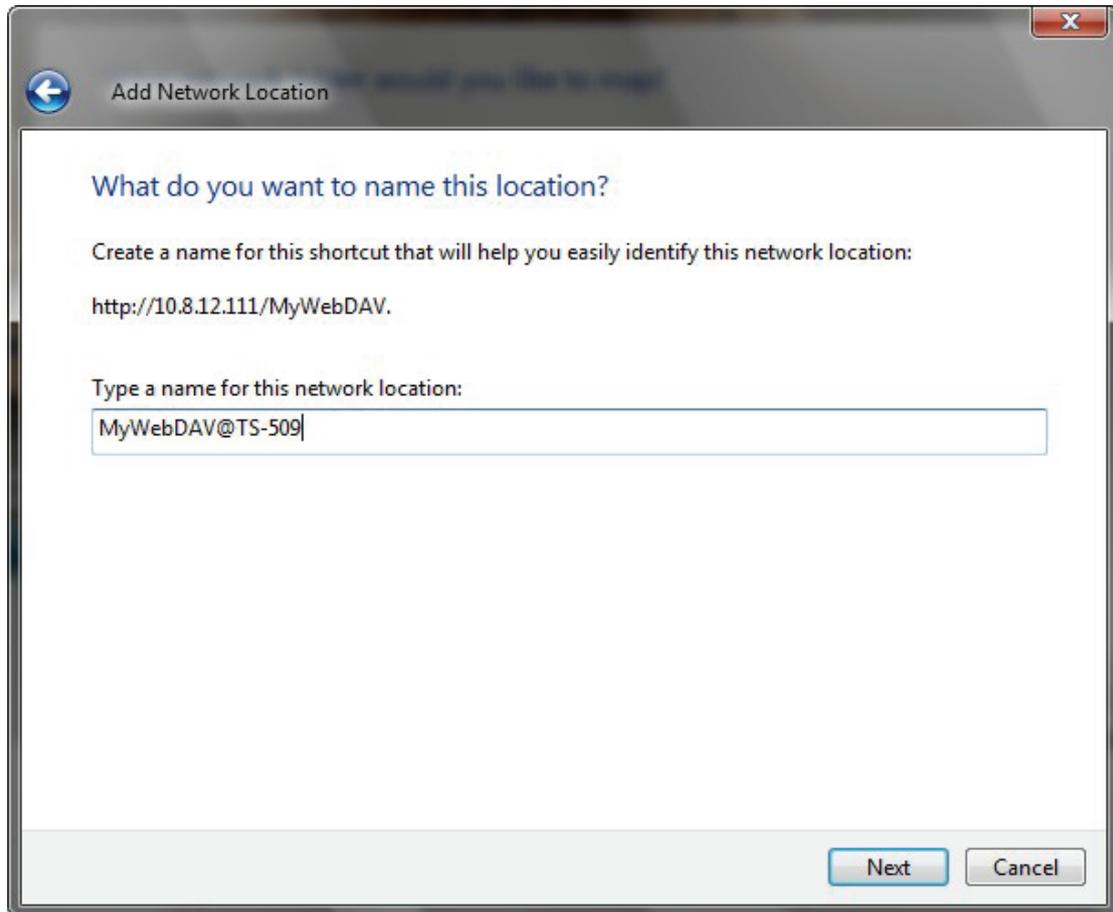


4. Enter the URL of your NAS with the share folder name.
Format: `http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME`

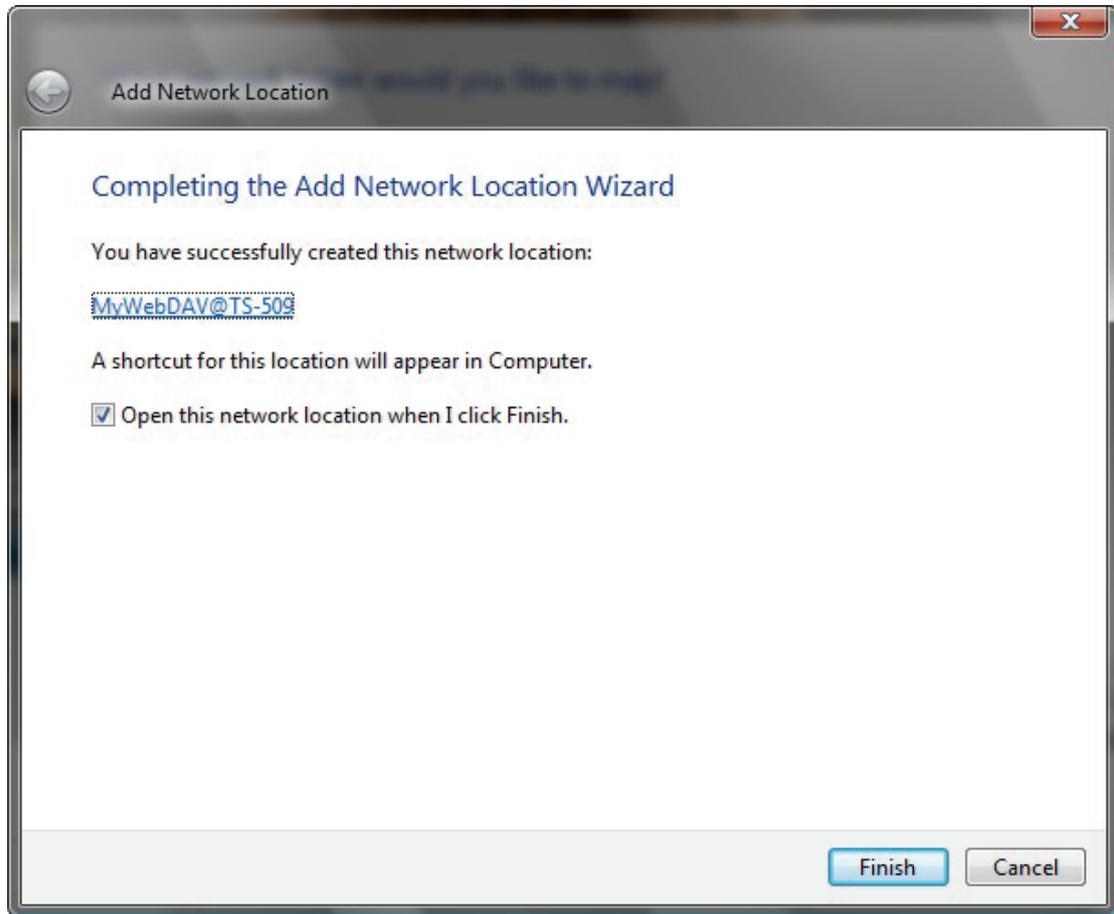


5. Enter the user name and password which has the WebDAV access right to connect to this share folder.

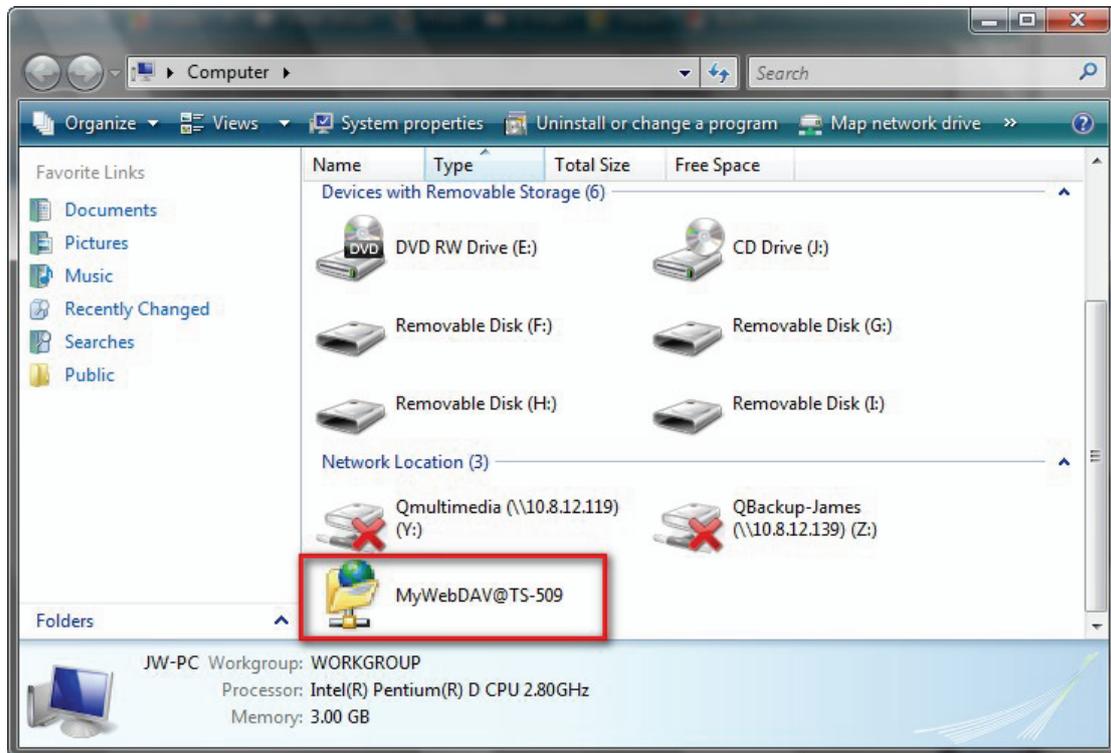
6. Type a name for this network location.



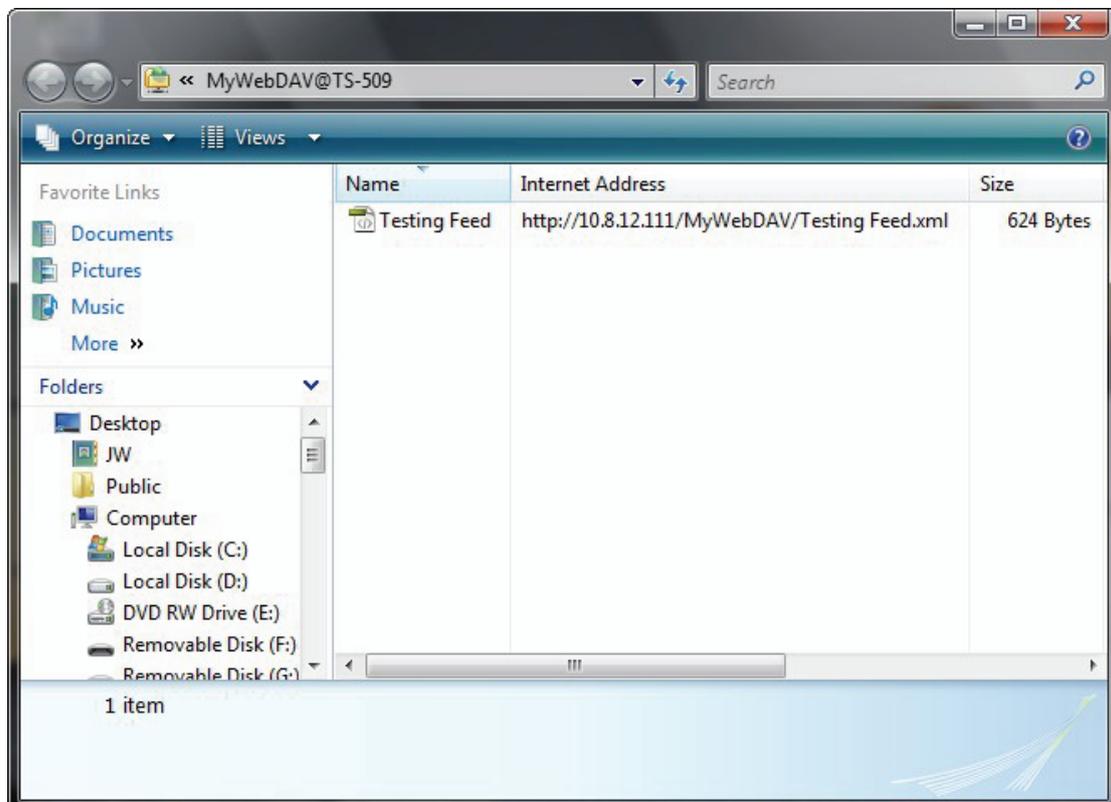
7. The Web folder has been successfully created.



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



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



Mac OS X

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

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

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



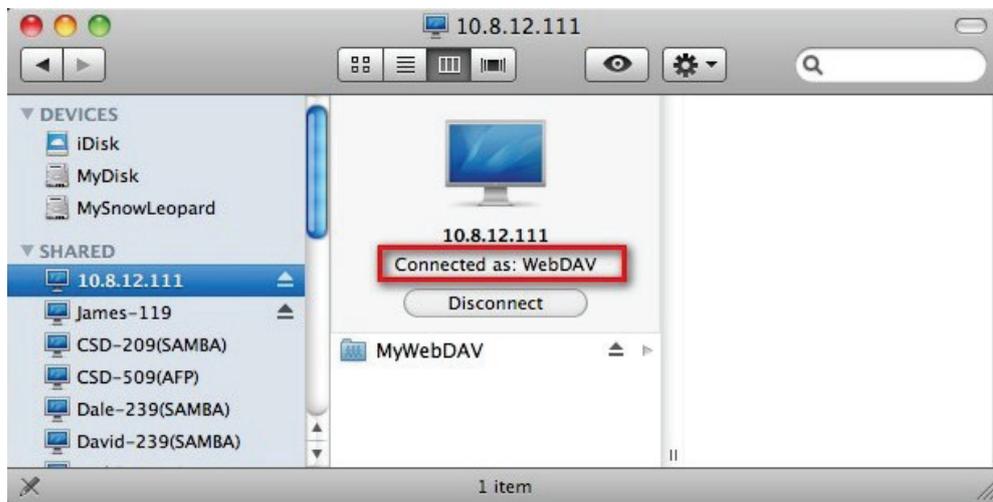
2. Enter the user name and password which has the WebDAV access right to connect to this share folder.



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



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



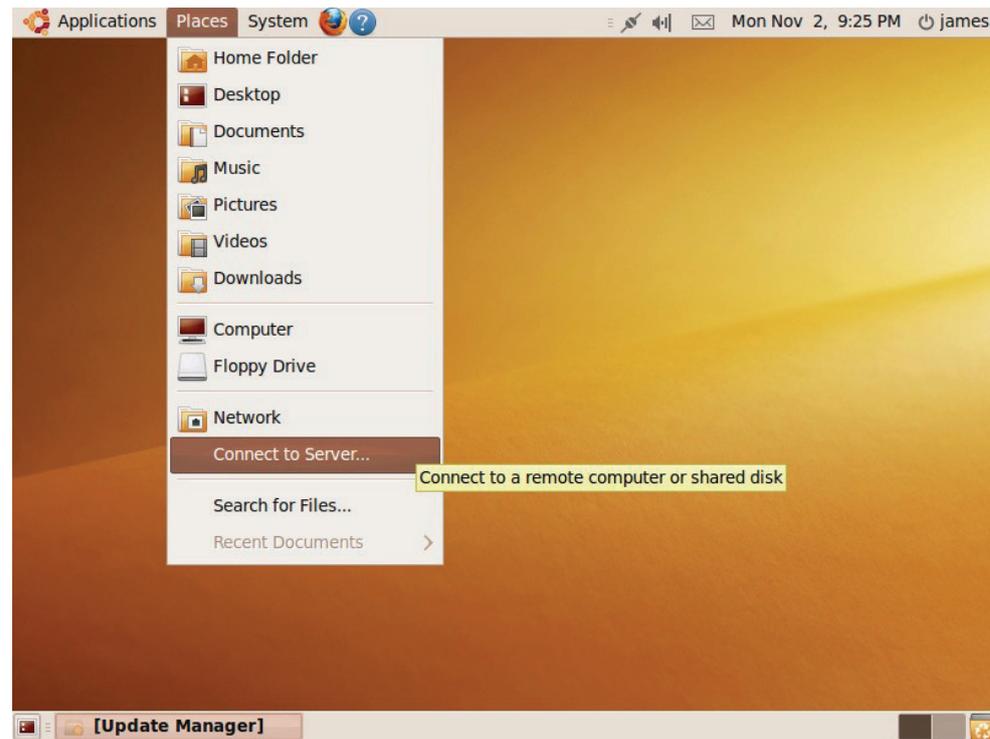
Note that the instructions above are based on Mac OS X 10.6, and can be applied to 10.4 or later.

Ubuntu

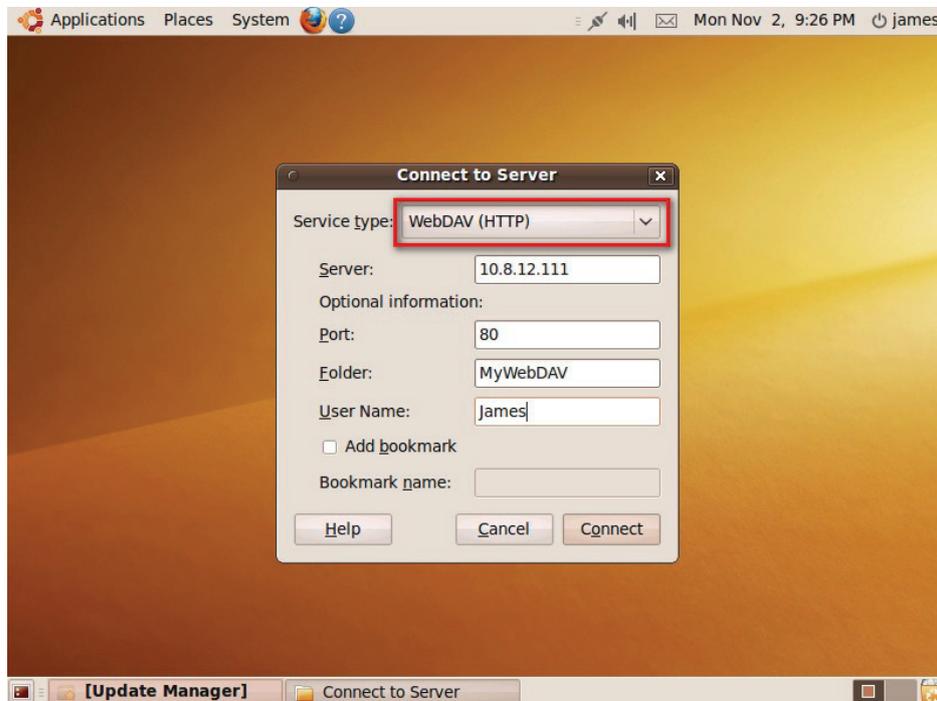
Follow the steps below to connect to your NAS via WebDAV on Ubuntu.

Client Operating System: Ubuntu 9.10 Desktop

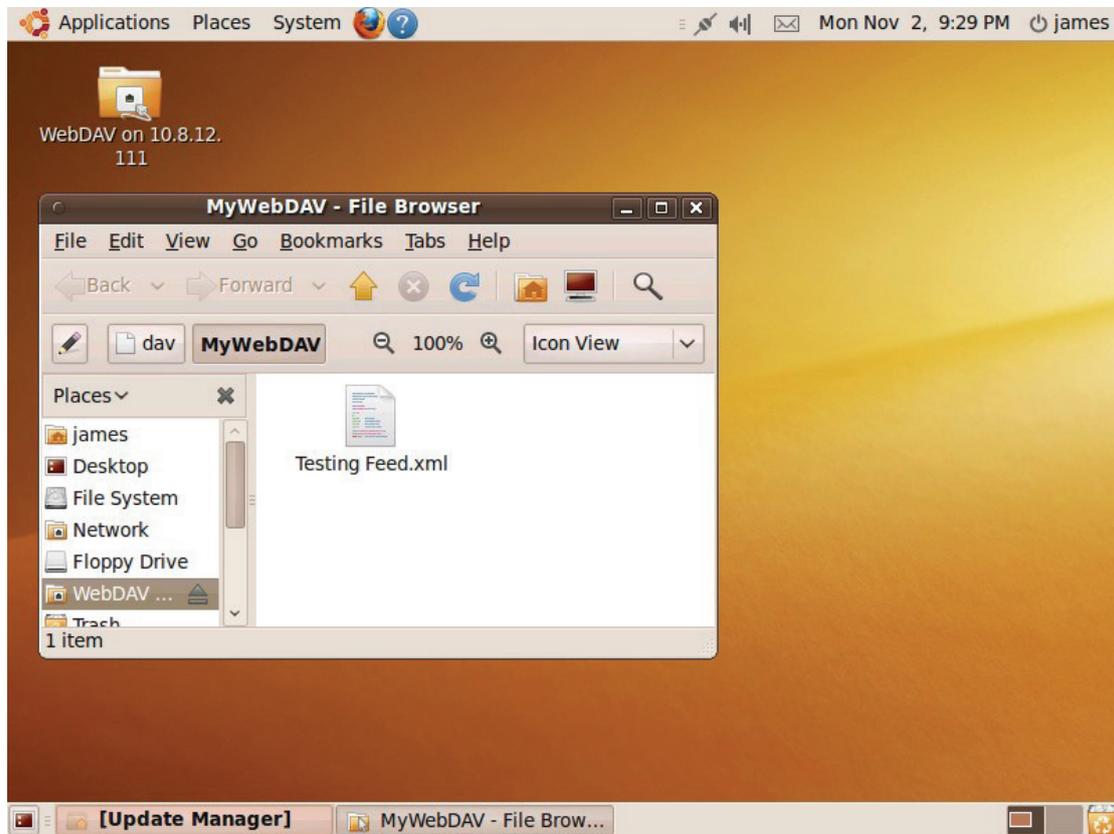
1. Open 'Places' > 'Connect to Server..'



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



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



MySQL Management

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

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

SQLite Management

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

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

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

[?]: The symbol '*' refers to the version number of SQLiteManager.

3.4.8 Network Service Discovery

3.4.8.1 UPnP Discovery Service

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

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



3.4.8.2 Bonjour

By broadcasting the network service(s) with Bonjour, your Mac will automatically discover the network services, 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.

UPNP DISCOVERY SERVICE **BONJOUR**

Bonjour

Before broadcasting the following services through Bonjour, please DO NOT forget to enable these services first.

- Web Administration
Service Name: QTP-TS639
- SAMBA (Server Message Block over TCP/IP)
Service Name: QTP-TS639(SAMBA)
- AFP (Apple File Protocol over TCP/IP)
Service Name: QTP-TS639(AFP)
- SSH
Service Name: QTP-TS639(SSH)
- FTP (File Transfer Protocol)
Service Name: QTP-TS639(FTP)
- HTTPS (Secure web server)
Service Name: QTP-TS639(HTTPS)
- UPNP (DLNA media server)
Service Name: QTP-TS639(UPNP)

3.5 Applications



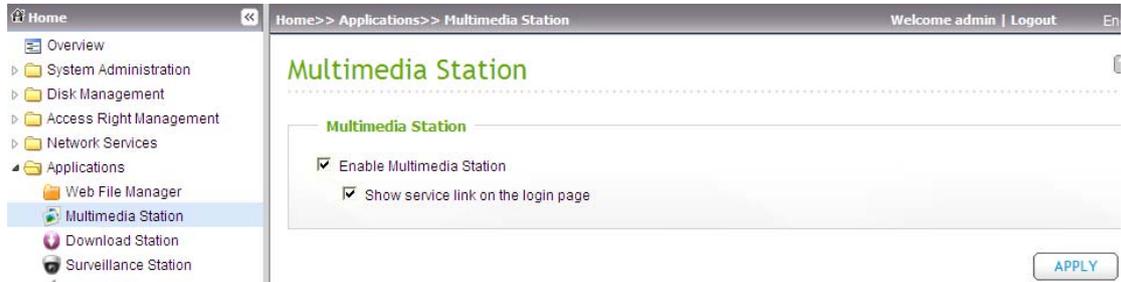
3.5.1 Web File Manager

To connect to the files on the NAS by a web browser, enable Web File Manager. If the NAS is connected to the Internet and uses a valid IP address, you can connect to the NAS by web browser from anywhere. For more information, see [Chapter 6](#).



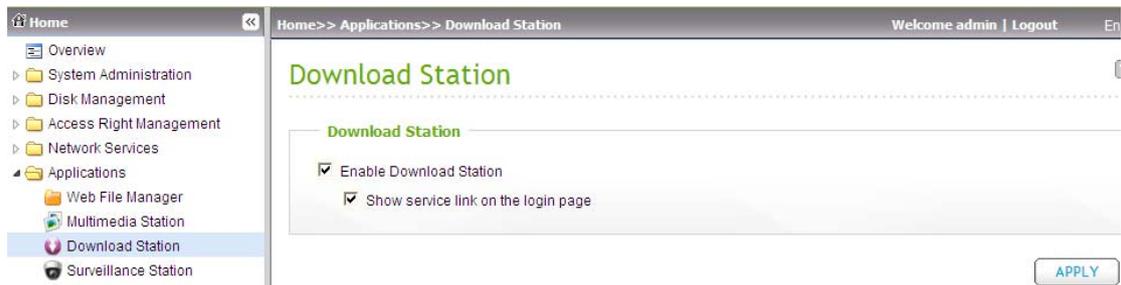
3.5.2 Multimedia Station

To share the photos, music, and video files on the NAS over the network, enable Multimedia Station. For further information of using Multimedia Station, iTunes service, and UPnP Media Server, see [Chapter 4](#).



3.5.3 Download Station

The NAS supports PC-less BT, HTTP, and FTP download. To use the download function of the NAS, enable Download Station. For further information, see [Chapter 5](#).



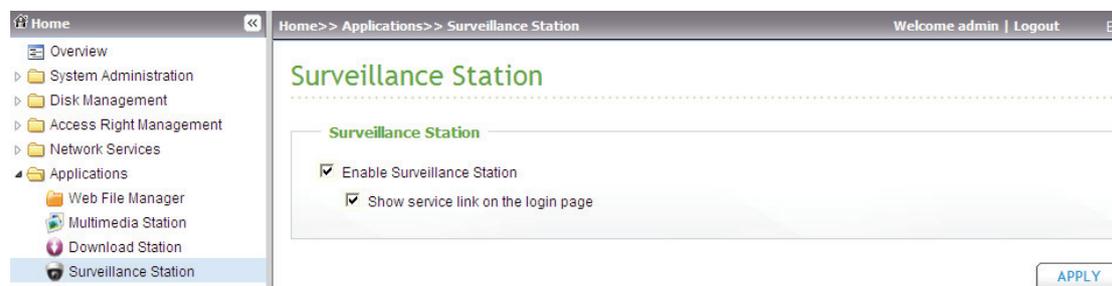
Important: Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions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

3.5.4 Surveillance Station

You monitor and record the live video of maximum 2-4 IP cameras available on the network (LAN or WAN) with Surveillance Station.

Maximum number of IP cameras	NAS models
2	TS-110, TS-119, TS-210, TS-219, TS-219P, S-239 Pro, TS-239 Pro II, TS-259 Pro
4	TS-410, TS-419P, TS-410U, TS-419U, SS-439 Pro, TS-439 Pro, TS-439 Pro II, TS-439U-SP/RP, TS-459 Pro, TS-459U-SP/RP, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, TS-809U-RP

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/>.



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

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

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

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

1. Plan your home network topology

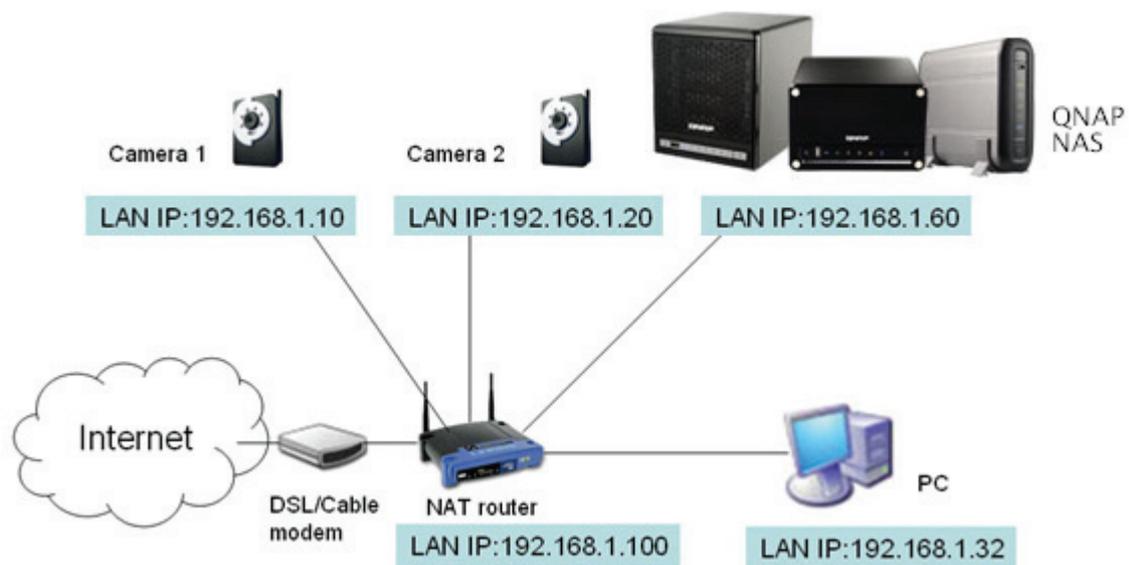
Write down your plan of the home network before setting up the surveillance system.

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)



2. Set up the IP cameras

In this example, two IP cameras will be installed. Connect the IP cameras to your home network. Then set the IP address of the cameras so that they are in the same LAN as the computer. Login the configuration page of the Camera 1 by IE browser.

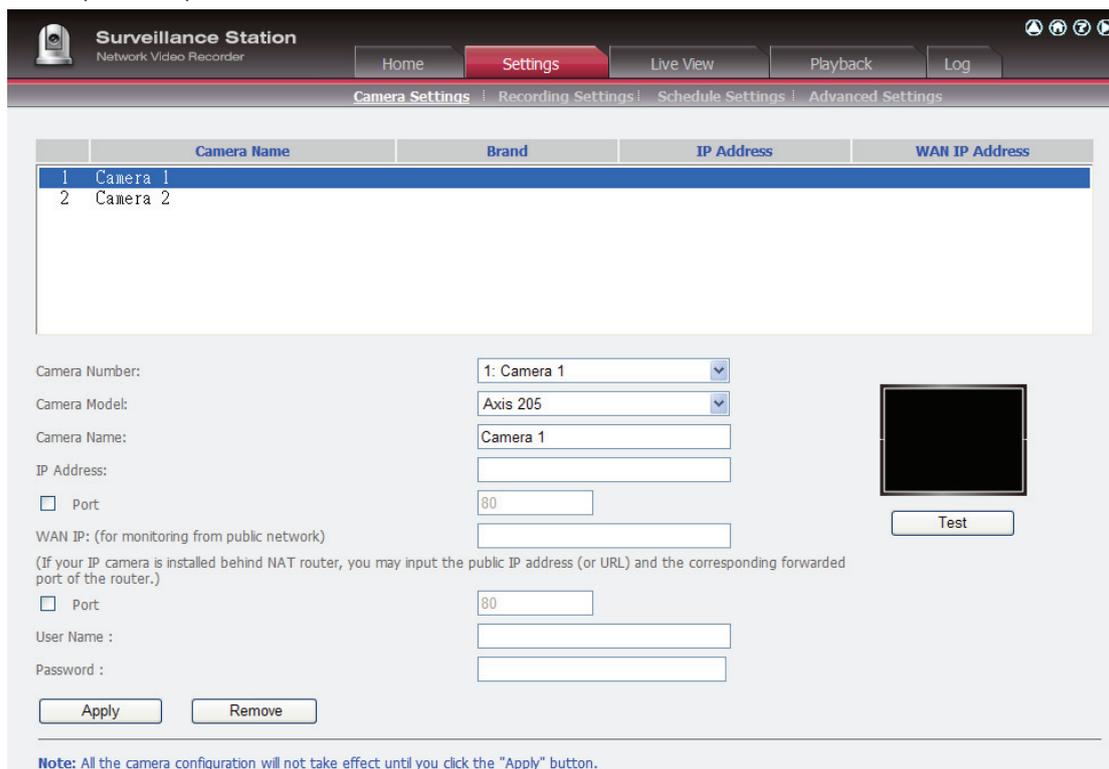
Enter the IP address of the first IP camera as 192.168.1.10. The default gateway should be set as the LAN IP of the router (192.168.1.100 in this example). Then configure the IP address of the second IP camera as 192.168.1.20.

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.

3. 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 with the 'Settings' tab selected. Under 'Camera Settings', there is a table with the following data:

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

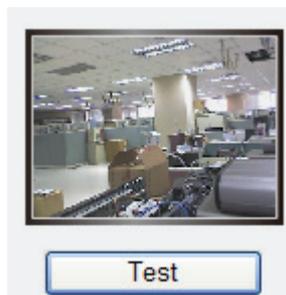
Below the table is a configuration form for 'Camera 1':

- Camera Number: 1: Camera 1 (dropdown)
- Camera Model: Axis 205 (dropdown)
- Camera Name: Camera 1 (text input)
- IP Address: (text input)
- Port: 80 (text input)
- WAN IP: (for monitoring from public network) (text input)
- (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 (text input)
- User Name: (text input)
- Password: (text input)

Buttons: Apply, Remove, Test (next to a video preview window).

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.

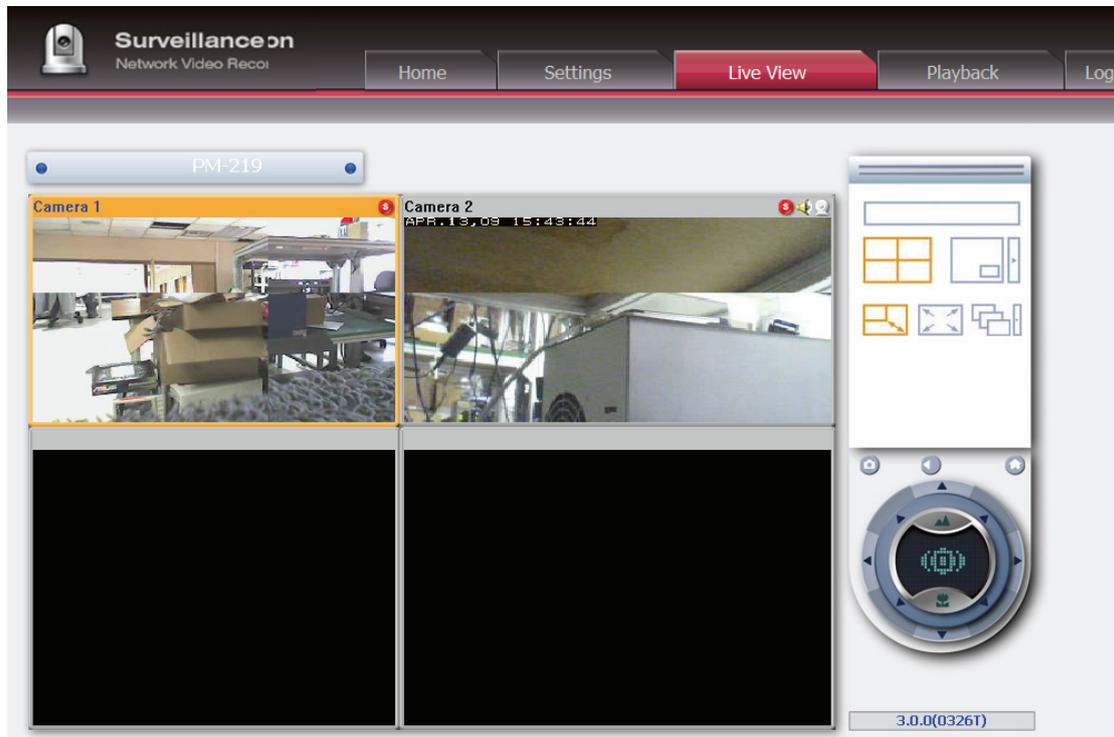
Camera Number:	2: Camera 2
Video Compression:	Motion JPEG
Resolution:	QVGA
Frame Rate:	20
Quality:	Normal
<input checked="" type="checkbox"/> Enable audio recording on this camera	
Estimated Storage Space for Recording: 6760 GB	
<input type="button" value="Apply"/>	

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.

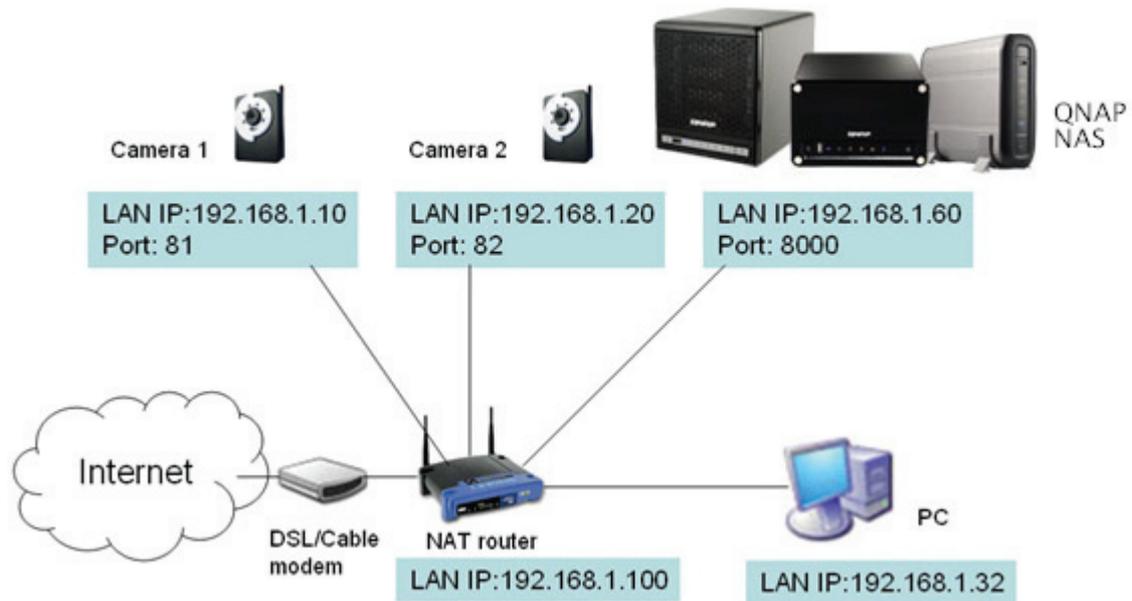
The first time you connect to this page by the IE browser, you have to install the ActiveX control in order to view the images of IP camera 1 and IP camera 2. You can start to use the monitoring and recording functions of the Surveillance Station.

To use other functions such as motion detection recording, scheduled recording, and video playback, see the online help.



4. 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.

The screenshot shows the 'Camera Settings' configuration page for 'Camera 1'. The fields are as follows:

- Camera Number: 1: Camera 1 (dropdown)
- Camera Model: iPUX ICS 1003/1013 (dropdown)
- Camera Name: Camera 1 (text input)
- IP Address: 192.168.1.10 (text input)
- Port: Port, 81 (text input)
- WAN IP: (for monitoring from public network) myNAS.dyndns.org (text input)
- Port: Port, 81 (text input)
- User Name: administrator (text input)
- Password: •••••• (password field)

Buttons: Apply, Remove, Test (next to a camera preview window).

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:

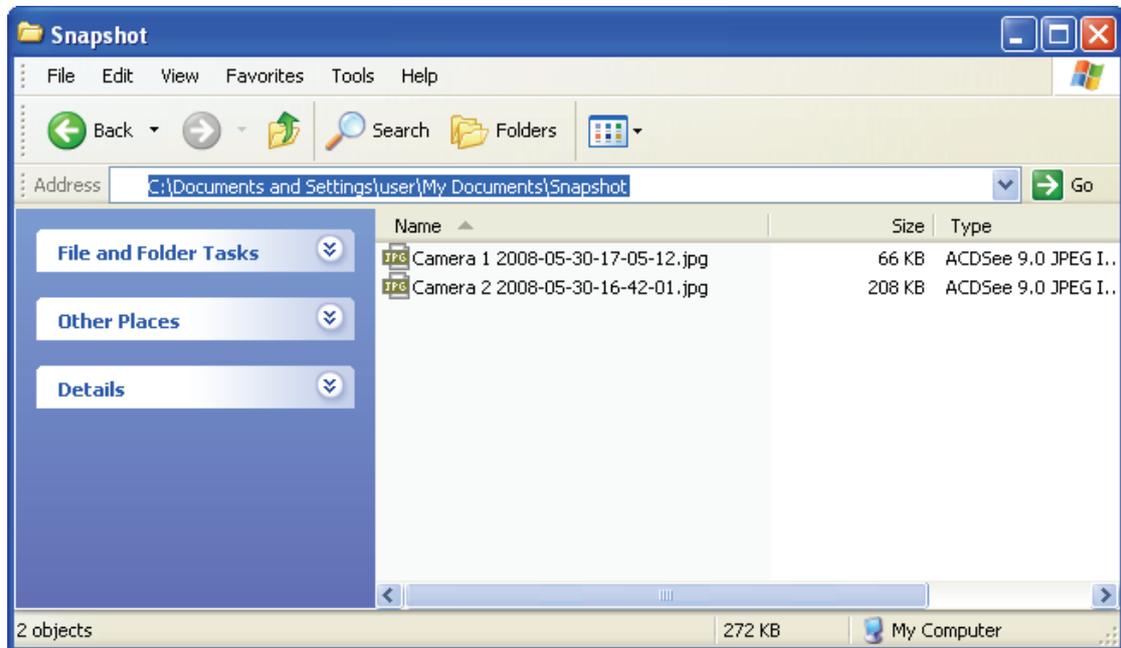
- Forward port 8000 to the LAN IP of the NAS: 192.168.1.60
- Forward port 81 to the LAN IP of IP camera 1: 192.168.1.10
- Forward port 82 to the LAN IP of IP camera 2: 192.168.1.20

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'.



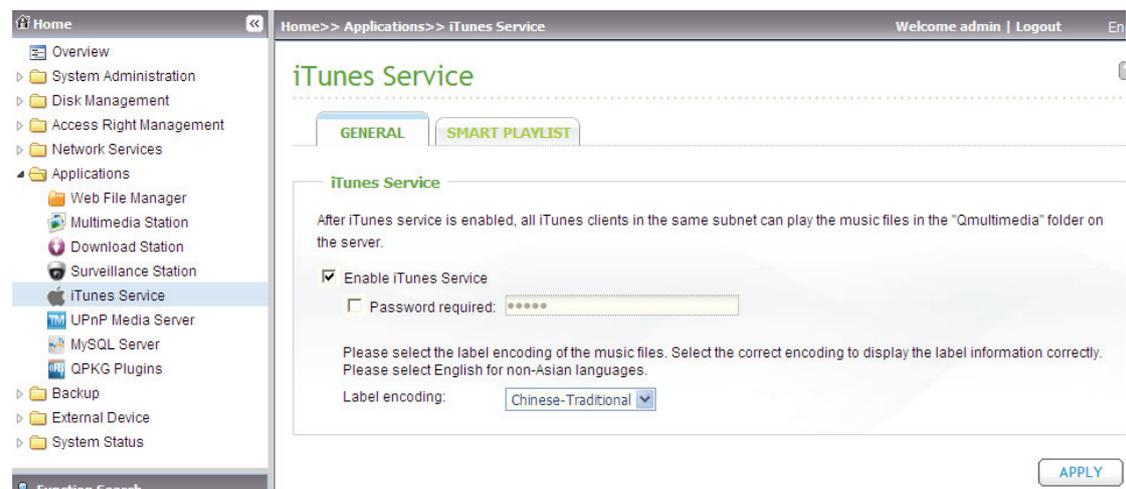
The video recordings will be saved in \\NASIP\Qrecordings or \\NASIP\Recordings.

The general recordings are saved in the folder 'record_nvr' and the alarm recordings are saved in the folder 'record_nvr_alarm'.

3.5.5 iTunes Service

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



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

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

iTunes Service ?

GENERAL
SMART PLAYLIST

Smart playlist - Add

Name:

▼

▼

+
-

CANCEL
APPLY

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



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



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

3.5.6 UPnP Media Server

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

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



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

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

After configuring the settings, you can upload MP3, photos, or video files to the specified share folders on the NAS.

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

For the information of setting up the UPnP media server of the NAS for media playing, see [Appendix D](#).

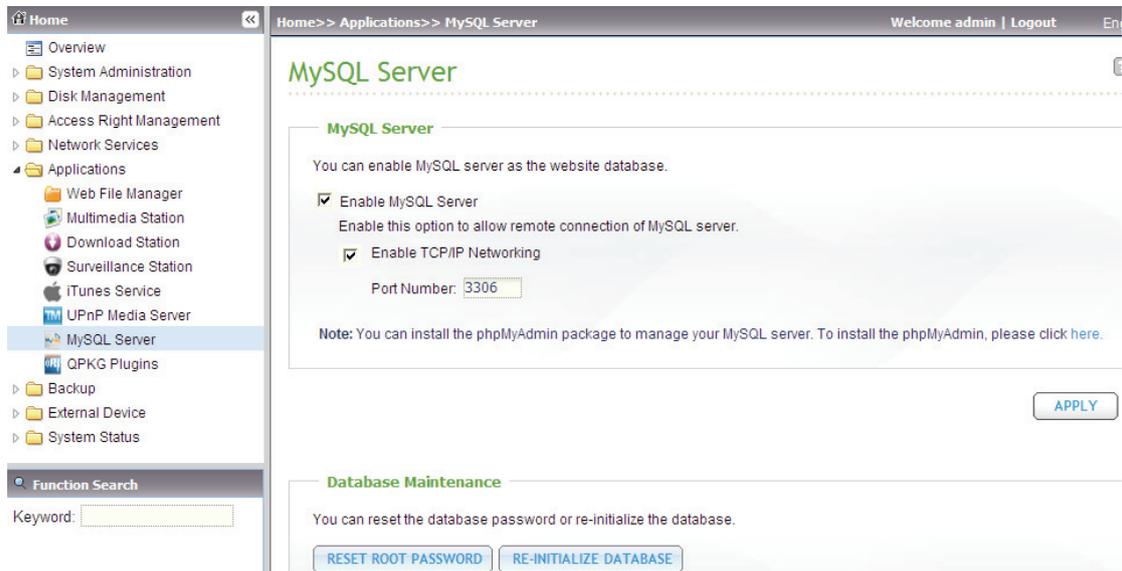
About UPnP and DLNA

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

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

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

3.5.7 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 [Appendix E](#).

3.5.8 QPKG Plugins

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

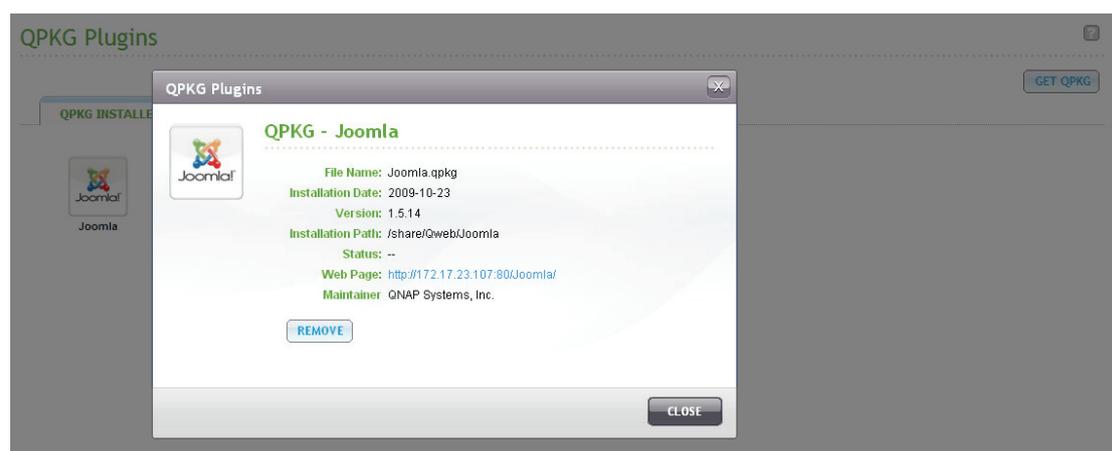


Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all the important data on the NAS. Download the package you want to install on the NAS to your computer.

Before installing the QPKG package, unzip the downloaded file. To install the QPKG, browse to select the correct QPKG file and click 'INSTALL'.

After uploading the QPKG packages, the details are shown. Click the link to connect to the web page of the installed package and start to configure the settings.

To remove the package from the NAS, click 'REMOVE'.



3.6 Backup



3.6.1 External Drive

You can back up the local drive data to an external storage device. Select to execute instant, automatic, or scheduled backup, and configure the settings.

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

Copy Options:

You can select 'Copy' to copy the files from the NAS to the external device. Select 'Synchronize' to synchronize the data between the NAS and the external storage device. Any differentiated files on the external device will be deleted.

Note: During the data copy or synchronization, the identical files on both sides will not be copied. If there are files in the same name but different in size or modified dates on NAS and the external device, the files on the external device are overwritten.

Home >> Backup >> External Drive Welcome admin | Logout

External Drive

Back up to an external storage device

Back up the local disk data to an external storage device. You can select instant, automatic, or schedule backup.

Directory to back up

- Qmultimedia
- Public
- 11

Directory not to back up

- Europe
- Network Recycle Bin 1
- Qdownload
- Qrecordings
- Qusb
- Qweb
- Users
- test
- video_demo

Back up to an External Storage Device: USBDisk1 No external device is detected currently.
 Free Size/Total Size:--

Backup Method: Backup Now Execute backup immediately.

Copy options: Copy Back up data to the destination drive.

Current Backup Status: No backup operations.

Last Backup Time:

Last Backup Result:

Function Search

Keyword:

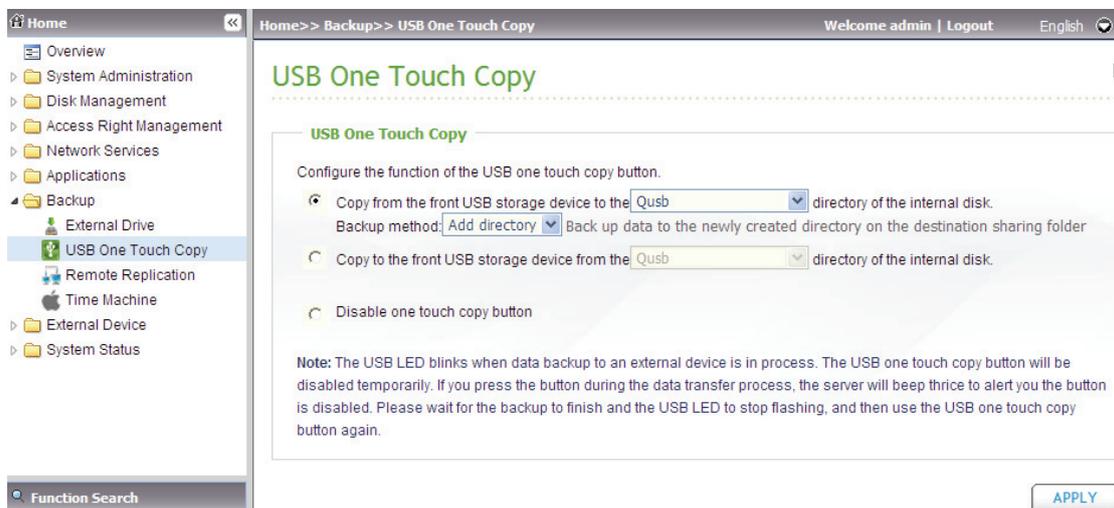
3.6.2 USB One Touch Copy

This feature is not supported by TS-809U-RP.

You can configure the behaviour of the USB one touch copy button on this page.

The following three functions are available:

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



Data Copy by the Front USB Port

The NAS supports instant data 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 HDD 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.

3.6.3 Remote Replication

3.6.3.1 Remote Replication

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

The maximum number of remote replication jobs supported is 64. Make sure a network share has been created before adding a remote replication task.

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

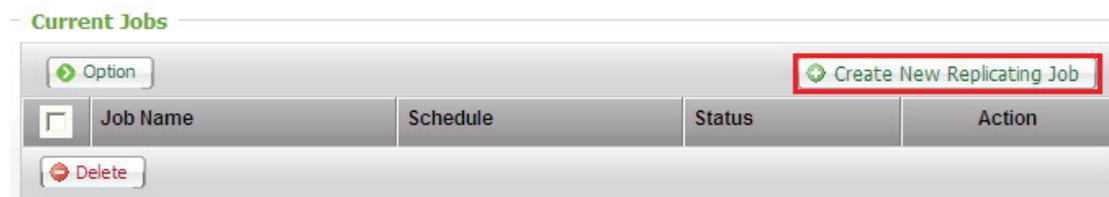
Note: If this server connects to the Internet through a router, make sure the specified port for remote replication is opened on the router.

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

The screenshot displays the QNAP web interface for Remote Replication. The left sidebar shows a navigation menu with 'Remote Replication' selected. The main panel is titled 'Remote Replication' and features two tabs: 'REMOTE REPLICATION' and 'AMAZON S3'. The 'REMOTE REPLICATION' tab is active, showing a description: '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.' Below this, there is a 'Port Number' field with the value '873'. Two checkboxes are present: 'Enable backup from a remote server to the local host' (checked) and 'Allow remote Rsync server to back up data to NAS' (unchecked). An 'APPLY' button is located at the bottom right of the configuration area. Below the configuration is a 'Current Jobs' section with a 'Delete' button and a 'Create New Replicating Job' button. A table with columns 'Job Name', 'Schedule', 'Status', and 'Action' is visible but empty.

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

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



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



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

Note:

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

Remote Replication X

QNAP
TURBO NAS

Remote Destination

Name or IP address of the remote server:

Port Number:

User Name:

Password:

Remote Host Testing:

Step 2 of 7

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

Remote Replication X

QNAP
TURBO NAS

Remote Destination

Destination Path :

(e.g. /ShareFolder/Directory)

Remain Capacity : 0 Mb

Step 3 of 7

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

The screenshot shows the 'Remote Replication' window for QNAP Turbo NAS. The title bar reads 'Remote Replication' with a close button. On the left is the QNAP logo. The main heading is 'Local Source'. Below it, the 'Local Path' is set to '/Public' in a text box, with an example '(e.g. /ShareFolder/Directory)' below. At the bottom, it says 'Step 4 of 7' and has 'BACK', 'NEXT', and 'CANCEL' buttons.

6. Define the replication schedule.

The screenshot shows the 'Remote Replication' window for QNAP Turbo NAS. The title bar reads 'Remote Replication' with a close button. On the left is the QNAP logo. The main heading is 'Replication Schedule'. Below it, 'Select schedule:' is followed by radio buttons for 'Replicate Now', 'Daily' (which is selected), 'Weekly', and 'Monthly'. To the right of these are dropdown menus for 'Monday', '01', and 'Time' (set to '00 : 00'). At the bottom, it says 'Step 5 of 7' and has 'BACK', 'NEXT', and 'CANCEL' buttons.

7. Set other options for the remote replication job. Then 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.

The screenshot shows the 'Remote Replication' window at Step 6 of 7. The title bar reads 'Remote Replication' with a close button. On the left is the QNAP TURBO NAS logo. The main area is titled 'Replication Options' and contains several checkboxes: 'Enable encryption, port number: 22', 'Activate file compression', 'Stop network file services while replicating', 'Perform incremental replication', 'Delete extra files on remote destination', and 'Handle sparse files efficiently'. A red note states: '(Note: You have to enable SSH connection on the remote host, and use the "admin" account to execute the encrypted replication job. Besides, the port number must be the same as the SSH port of the remote host.)'. At the bottom, there are 'Step 6 of 7' and buttons for 'BACK', 'NEXT', and 'CANCEL'.

Remote Replication

QNAP
TURBO NAS

Replication Options

- Enable encryption, port number: 22
- Activate file compression
- Stop network file services while replicating
- Perform incremental replication
- Delete extra files on remote destination
- Handle sparse files efficiently

(Note: You have to enable SSH connection on the remote host, and use the "admin" account to execute the encrypted replication job. Besides, the port number must be the same as the SSH port of the remote host.)

Step 6 of 7

BACK NEXT CANCEL

The screenshot shows the 'Remote Replication' window at Step 7 of 7. The title bar reads 'Remote Replication' with a close button. On the left is the QNAP TURBO NAS logo. The main area is titled 'Setup complete' and contains the text: 'The remote replication settings have been completed. Click FINISH to exit the Wizard.' At the bottom, there are 'Step 7 of 7' and a 'FINISH' button.

Remote Replication

QNAP
TURBO NAS

Setup complete

The remote replication settings have been completed. Click **FINISH** to exit the Wizard.

Step 7 of 7

FINISH

How to create a remote replication job for an entire disk volume?

To back up an entire disk volume by remote replication, create a new share folder (for example, root) as the root directory which contains all the share folders in the same volume, and specify the path to '/'. Then create a remote replication job to copy this share folder (root). All the share folders and sub-folders will be replicated.

The screenshot shows the 'Share Folder Property' dialog box. The 'Path' field is highlighted with a red box and contains the value '/'. Other fields include 'Network Share Name: root', 'Disk Volume: RAID 5 Disk Volume: Drive 1 2 3', 'Hide Network Drive: No', 'Lock file (oplocks): Yes', and 'Enable write-only access on FTP connection'.

Share Folder Property

Share Folder Property

Network Share Name: root

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

Hide Network Drive: Yes No

Lock file (oplocks): Yes No

Path: /

Comment (optional):

Enable write-only access on FTP connection

Step 1 of 1

APPLY CANCEL

3.6.3.2 Amazon S3

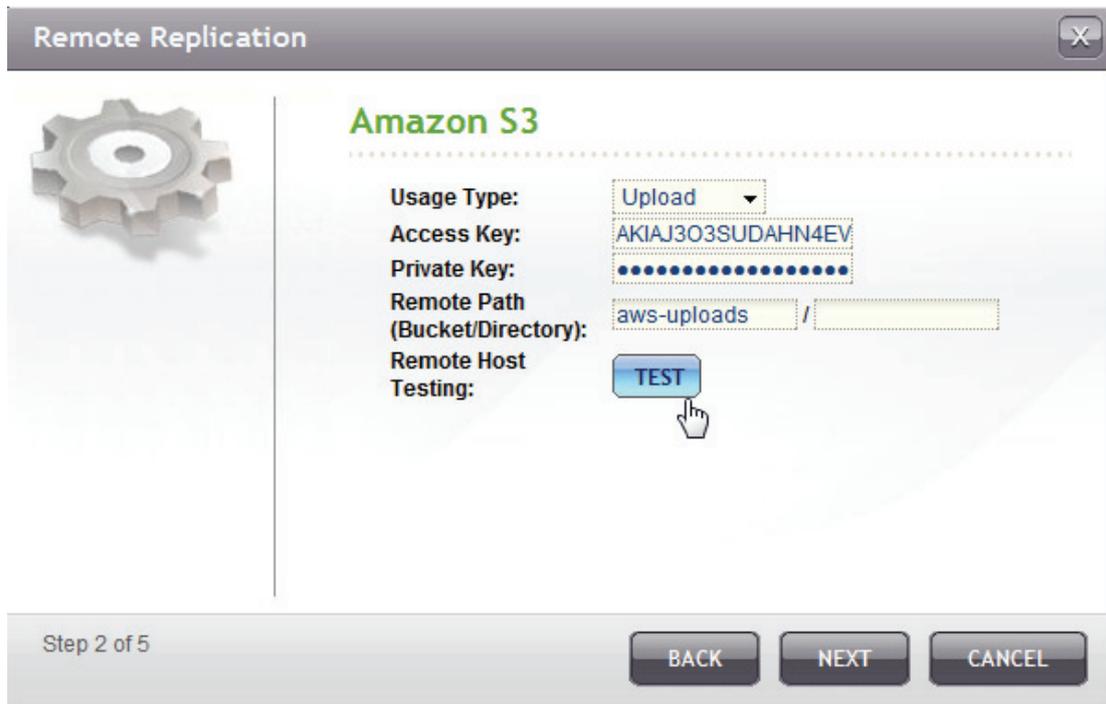
Amazon S3 (Simple Storage Service) is an online storage web service offered by AWS (Amazon Web Services). It provides a simple web services interface that can be used to store and retrieve the data from anywhere on the web. With Amazon S3, you can upload the data from your NAS to Amazon S3 or download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

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

The screenshot shows a web interface with two tabs: 'REMOTE REPLICATION' and 'AMAZON S3'. The 'AMAZON S3' tab is active. Below the tabs, there is a section titled 'Amazon S3' with the text: 'This function allows you to upload the data from the NAS to Amazon S3, or vice versa.' Below this, a note states: '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](#).' Below the note, there is a section titled 'Current Jobs' with a button labeled 'Create New Replicating Job'. Below the button is a table with the following columns: 'Job Name', 'Usage Type', 'Schedule', 'Status', and 'Action'.

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.

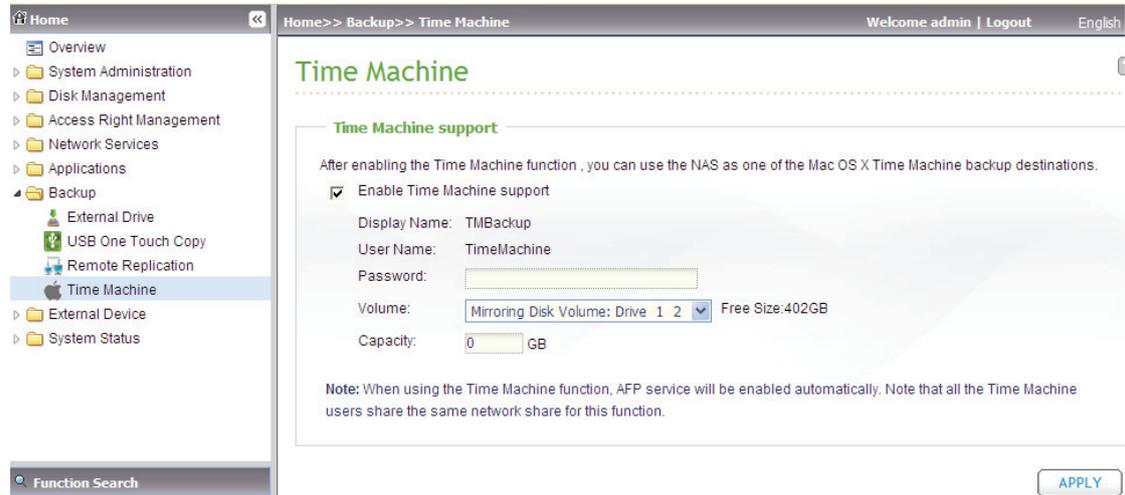
1. Click 'Create New Replicating Job'.
2. Enter the remote replication job name.
3. Select the usage type: 'Upload' or 'Download' and enter other settings. A bucket is the root directory on Amazon S3. You can test the connection to the remote host testing by clicking 'TEST'. Other settings are optional.



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.

3.6.4 Time Machine

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



To use this function, follow the steps below.

Configure the settings on the NAS:

1. Enable Time Machine support.

Time Machine

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: Free Size:402GB

Capacity: GB

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.

[APPLY](#)

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

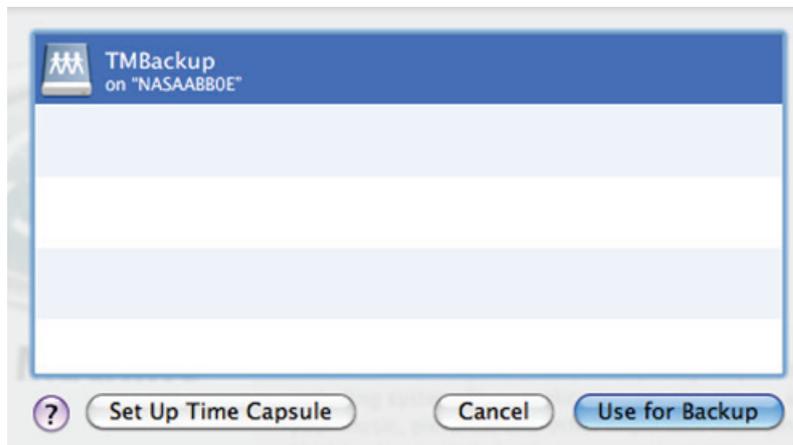
All the Time Machine users share the same network share for this function.

Configure the backup settings on Mac:

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



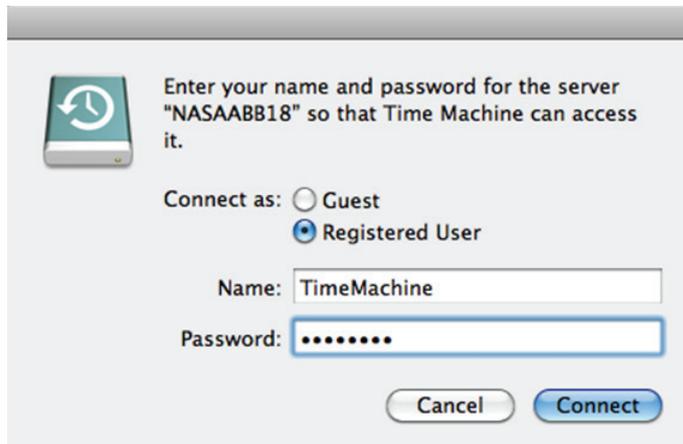
2. Select the TMBBackup on your NAS from the list and click 'Use for Backup'.



3. Enter the user name and password to login the QNAP NAS. Then click 'Connect'.

Registered user name: TimeMachine

Password: The password you have configured on the NAS. The password is empty by default.



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



The first time backup may take 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/>.

3.7 External Device



3.7.1 External Storage Device

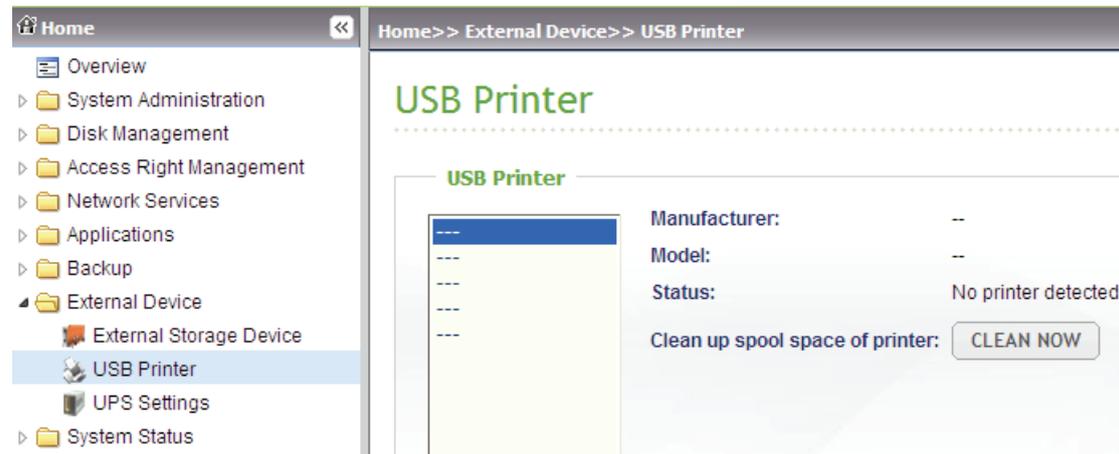
The NAS supports USB disks and thumb drives for extended storage. Connect the USB device to the USB port of the NAS, when the device is successfully detected, the details are shown on this page.

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



3.7.2 USB Printer

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



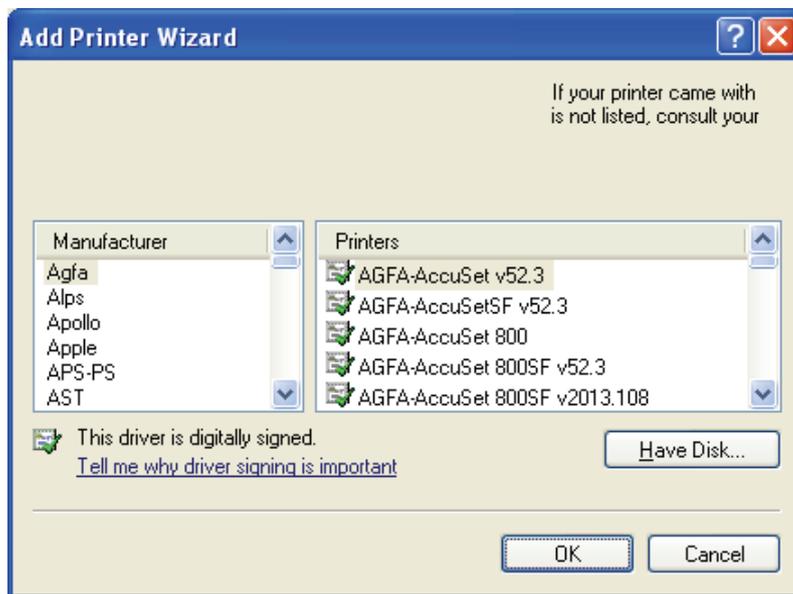
Note:

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

3.7.2.1 *Windows XP Users*

Method 1

1. Enter \\WAS 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.

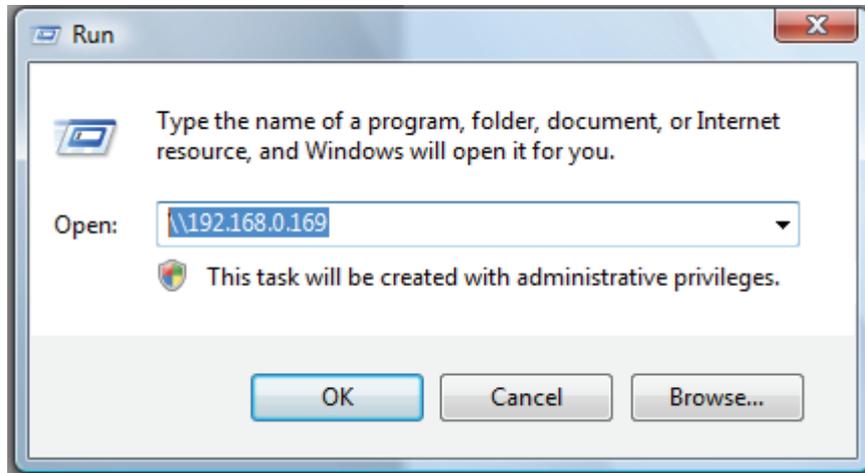
Method 2

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.

3.7.2.2 Windows Vista/ Windows 7 Users

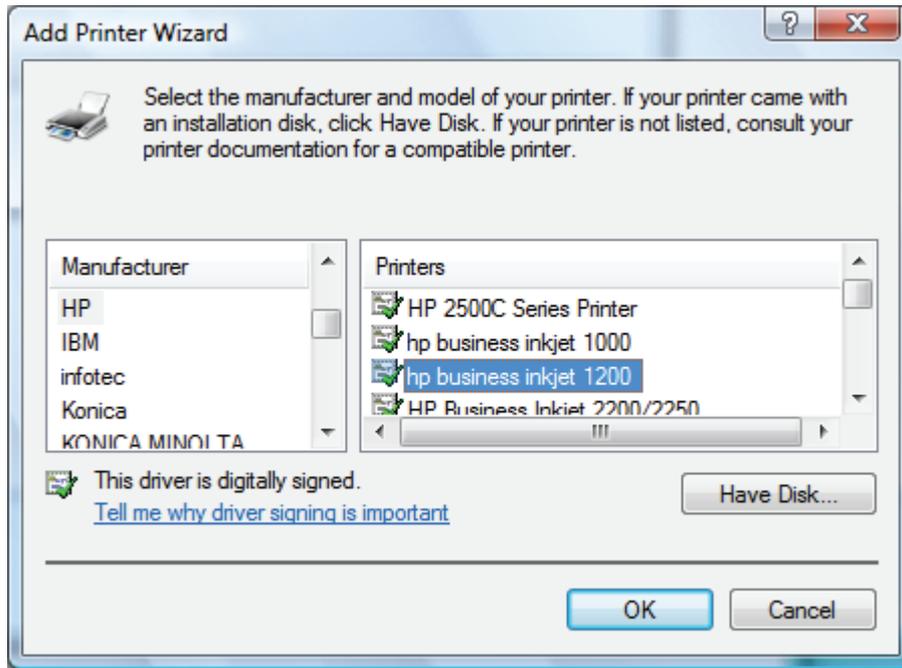
1. On the Run menu, enter \\NAS IP.



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



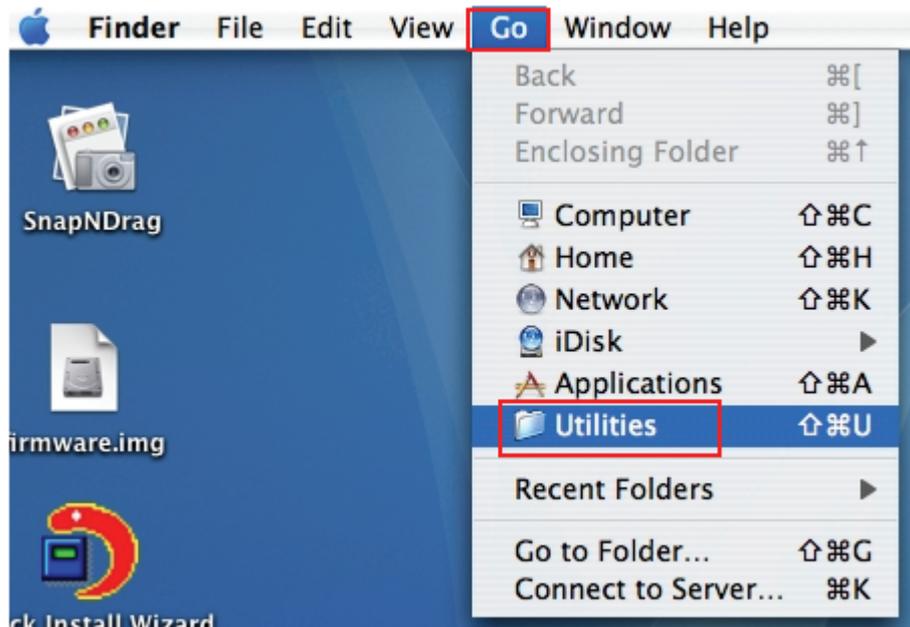
3. Install the correct printer driver.



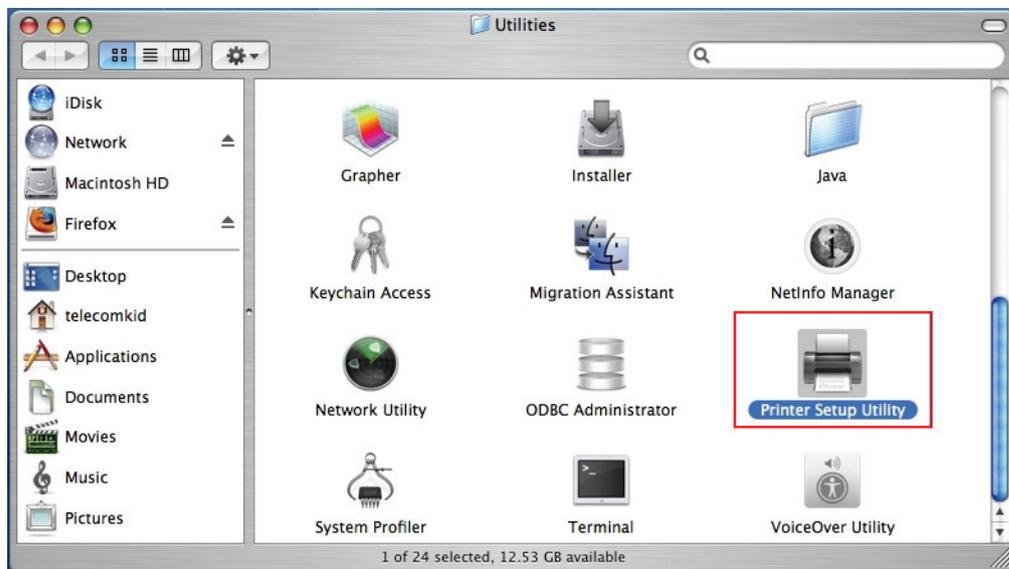
4. When finished, print a test page to verify the printer is ready to use.

3.7.2.3 Mac OS X 10.4

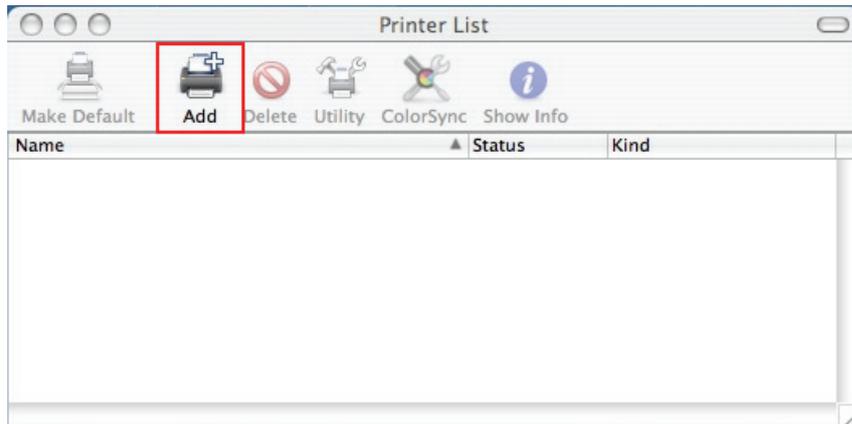
1. On the toolbar, click 'Go/ Utilities'.



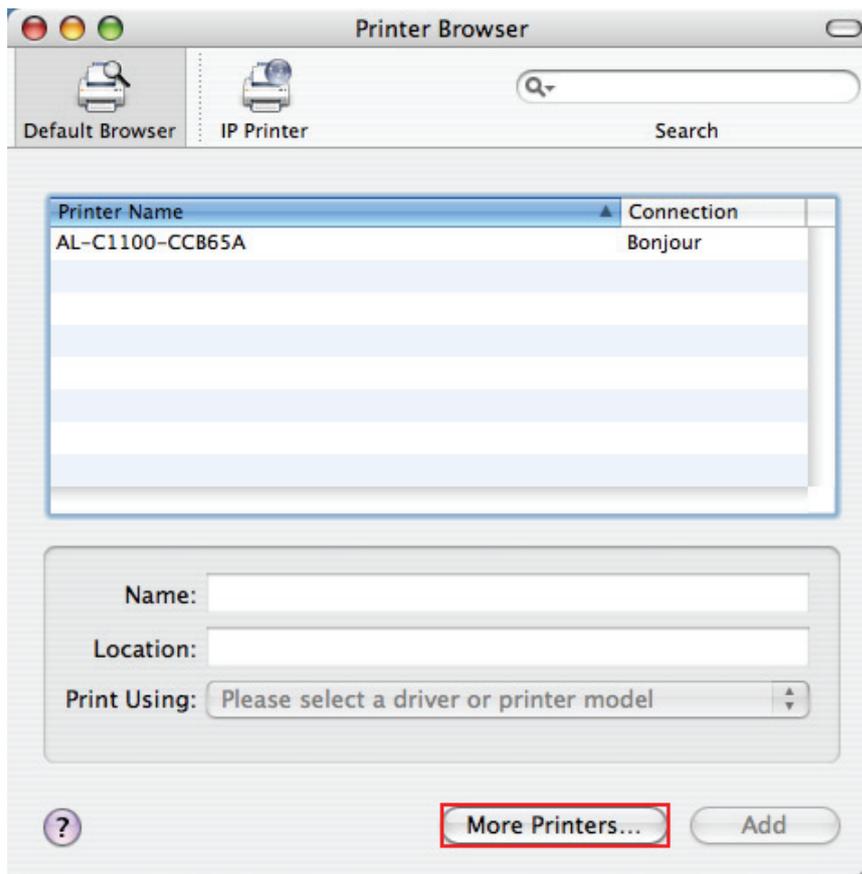
2. Click 'Printer Setup Utility'.



3. Click 'Add'.



4. Press and hold the 'alt' key  on the keyboard and click 'More Printers' concurrently.



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



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

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

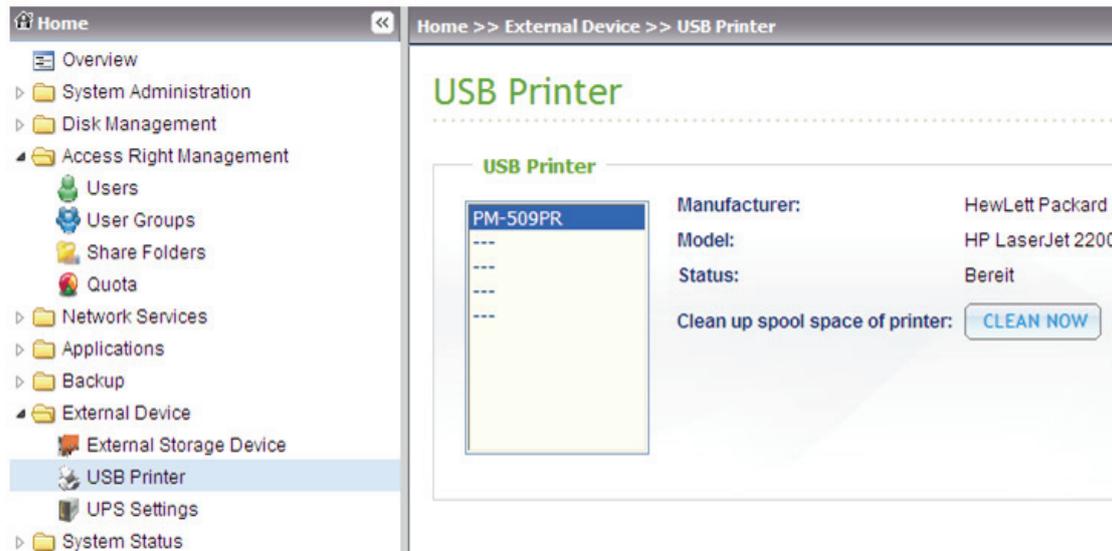


Note: The network printer service of the NAS supports Postscript printer on Mac OS only.

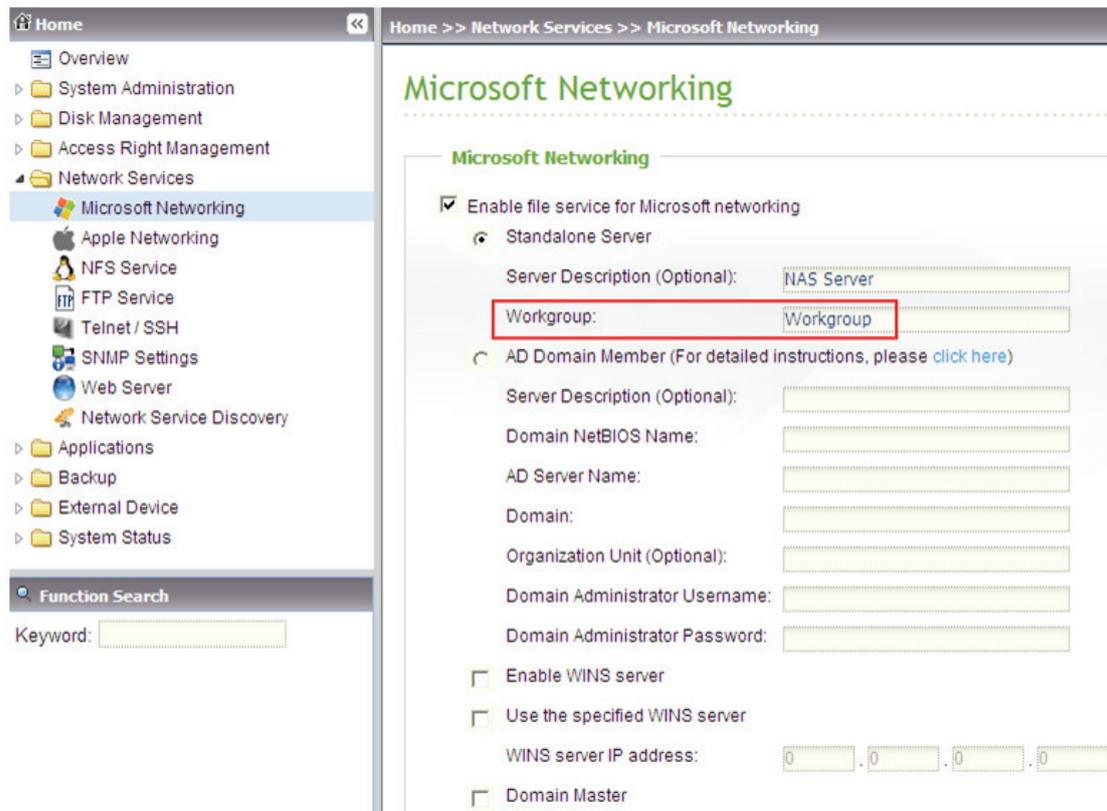
3.7.2.4 Mac OS X 10.5

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

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



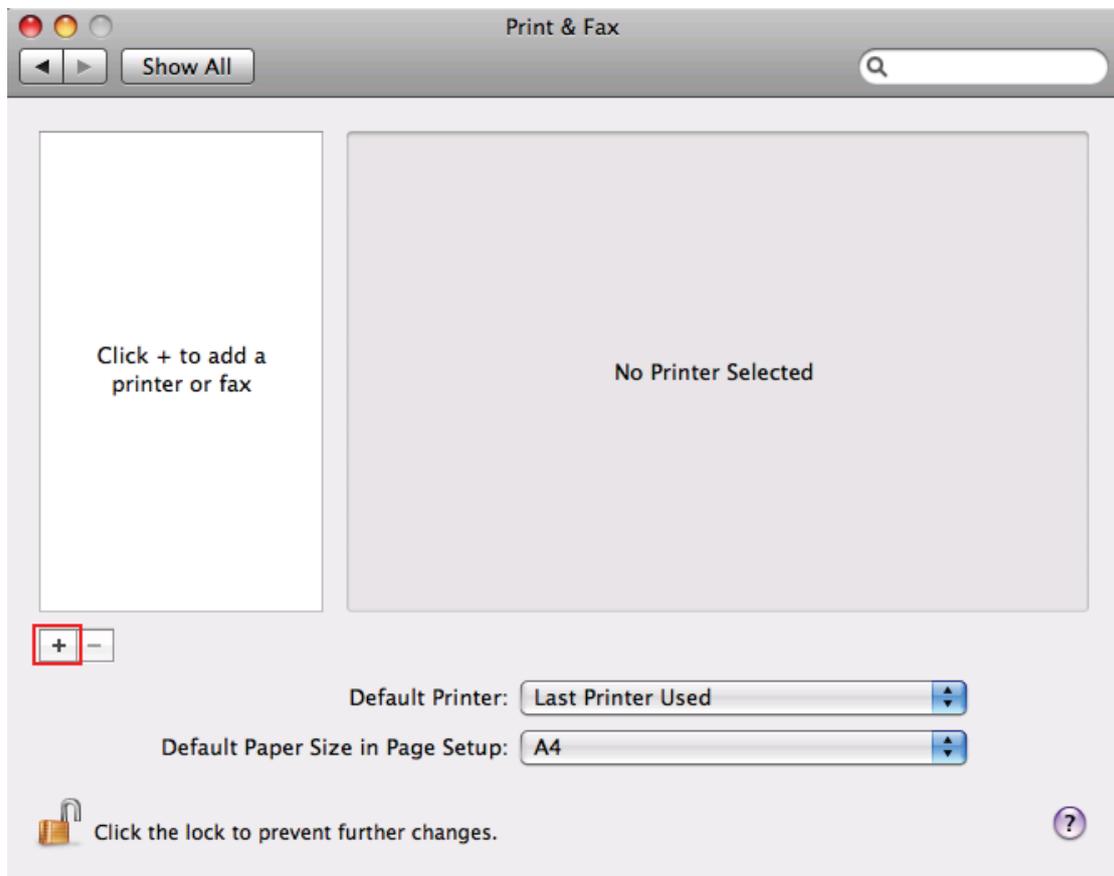
- Go to 'Network Services' > 'Microsoft Networking'. Enter a workgroup name for the NAS. You will need this information later.



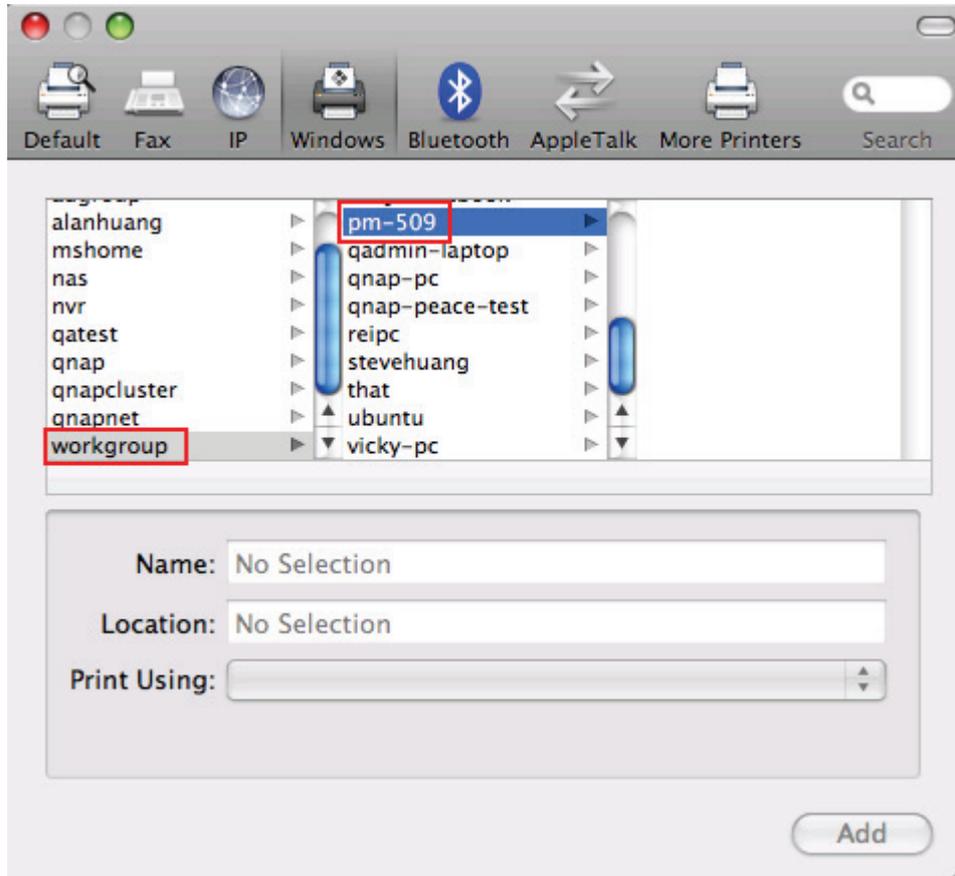
- Go to 'Print & Fax' on your Mac.



4. Click + to add a printer.



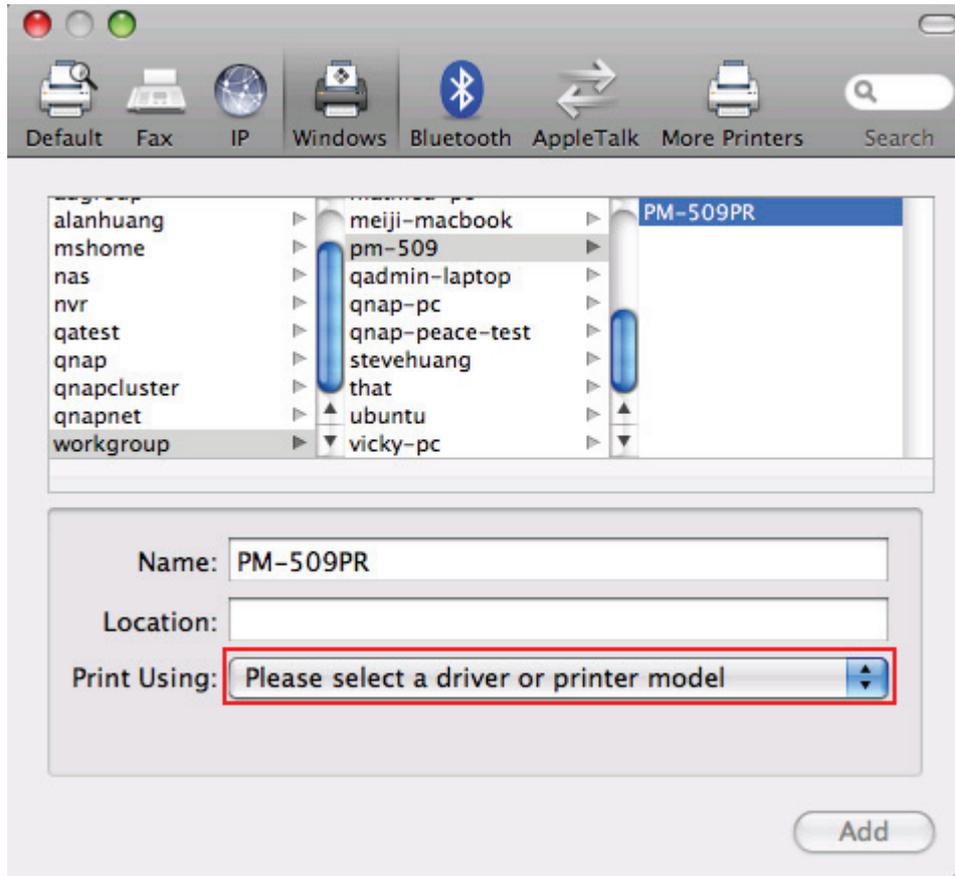
5. Select the NAS workgroup and find the printer name.



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



7. Select the printer driver.



✓ Please select a driver or printer model

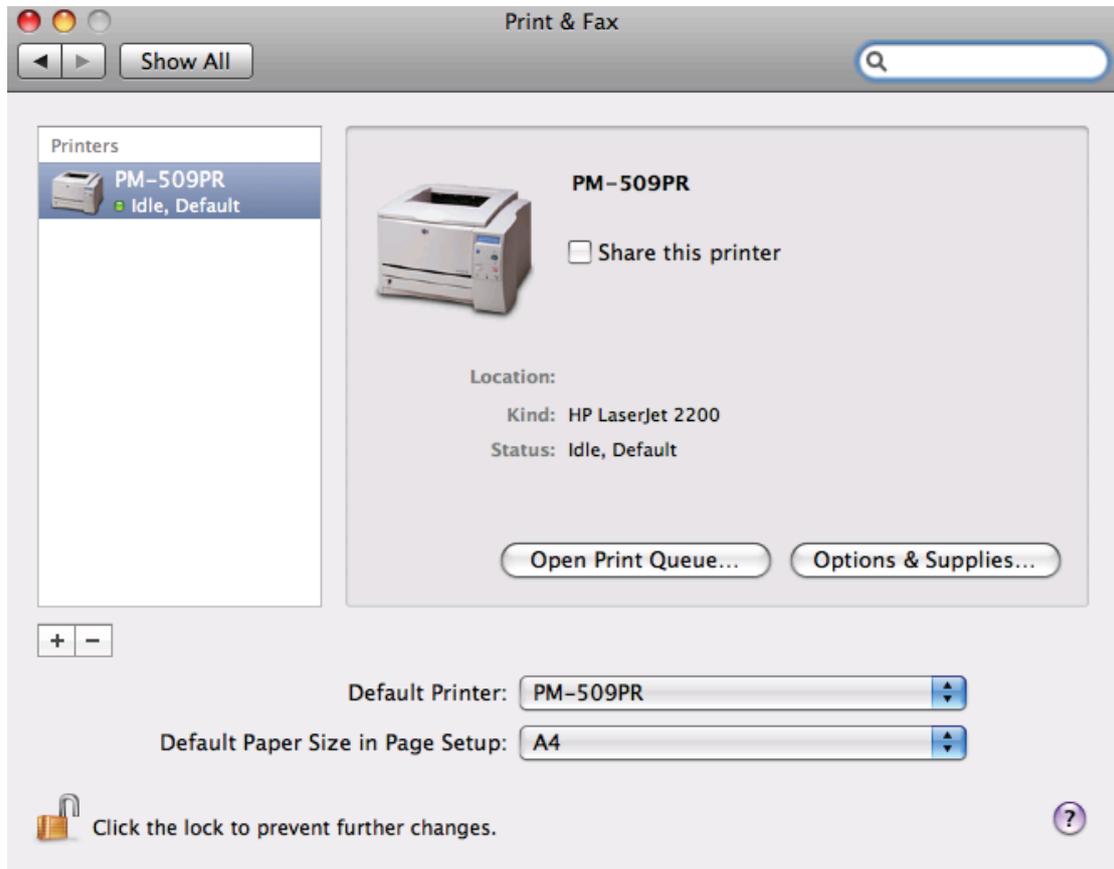
Auto Select

Generic PostScript Printer

Select a driver to use...

Other...

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



3.7.3 UPS Settings

You can connect a UPS (uninterruptible power supply) to the NAS and enable the UPS support. When an unexpected power outage occurs, the UPS is able to supply the power to the NAS continuously. You can also configure the settings to turn off the NAS after the AC power fails. If the power of the UPS is insufficient to last for the time specified, the NAS will shut down immediately for optimized server protection.

The screenshot shows the QNAP NAS web interface. The breadcrumb path is Home >> External Device >> UPS Settings. The left sidebar contains a navigation menu with 'UPS Settings' selected. The main content area is titled 'UPS Settings' and contains the following configuration options:

- Enable UPS Support
 - After the AC power fails for 5 minute(s), turn off the server.
 - After the AC power fails for 2 minute(s), the server should enter standby mode. When the power resumes, the system resumes to the operation status.
- UPS Model: USB UPS (auto detect)
- IP Address of UPS: 0 . 0 . 0 . 0

Below the settings is an 'UPS Information' section with the following fields:

- UPS Brand: --
- UPS Model: --
- AC Power Status: --
- Battery Capacity: --
- Estimated Protection Time: --

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

✓ Enable UPS support

Select this option to enable the UPS support. Enter the time the NAS should wait before shutting down after the AC power fails. In general, the UPS can supply the power for 5-10 minutes when the AC power fails depending on the maximum load and the number of connected devices.

✓ UPS Model

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

✓ IP Address of UPS

If you select to use 'APC UPS with SNMP Management', enter the IP address of the UPS.

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

Behaviour of the UPS feature of the NAS:

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

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

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

Once the power recovers:

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

Difference between standby mode and power-off mode

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

If the power recovers after the NAS has been shut down and before the UPS device is powered off, you may 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, and TS-419U.

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

The screenshot shows a web-based system administration interface. On the left is a navigation menu with a 'Home' icon and a back arrow. The menu items are: Overview, System Administration (expanded), General Settings, Network, Hardware, Security, Notification, Power Management (highlighted), Network Recycle Bin, Backup System Settings, System Logs, Firmware Update, Restore to Factory Default, Disk Management, Access Right Management, Network Services, Applications, and Backup. The main content area has a breadcrumb trail: Home >> System Administration >> Power Management. It contains three sections: 1. 'Restart/ Shutdown' with a button labeled 'Execute system restart/ shutdown immediately.' 2. 'Configure Wake on LAN' with two radio buttons: 'Enable' (unselected) and 'Disable' (selected). 3. 'When the AC power resumes:' (highlighted with a red box) with three radio buttons: 'Resume the server to the previous power-on or power-off status.' (selected), 'Turn on the server automatically.', and 'The server should remain off.'

3.8 System Status

Home >> System Status

System Status

- System Information
- System Service
- Resource Monitor

3.8.1 System Information

You can view the system information such as CPU usage and memory on this page.

Home >> System Status >> System Information

System Information

CPU Usage	6.7 %
Total Memory	1007.8 MB
Free Memory	794.0 MB
Ethernet 1 Packets Received	77269909
Ethernet 1 Packets Sent	63572520
Ethernet 1 Error Packets	0
Ethernet 2 Packets Received	0
Ethernet 2 Packets Sent	0
Ethernet 2 Error Packets	0
CPU Temperature	43°C/109°F
System Temperature	41°C/105°F
HDD 1 Temperature	42°C/107°F
HDD 2 Temperature	41°C/105°F
System Up Time	0 Day 20 Hour 4 Minute(s)
System Fan Speed	1229

Function Search
Keyword:

3.8.2 System Service

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

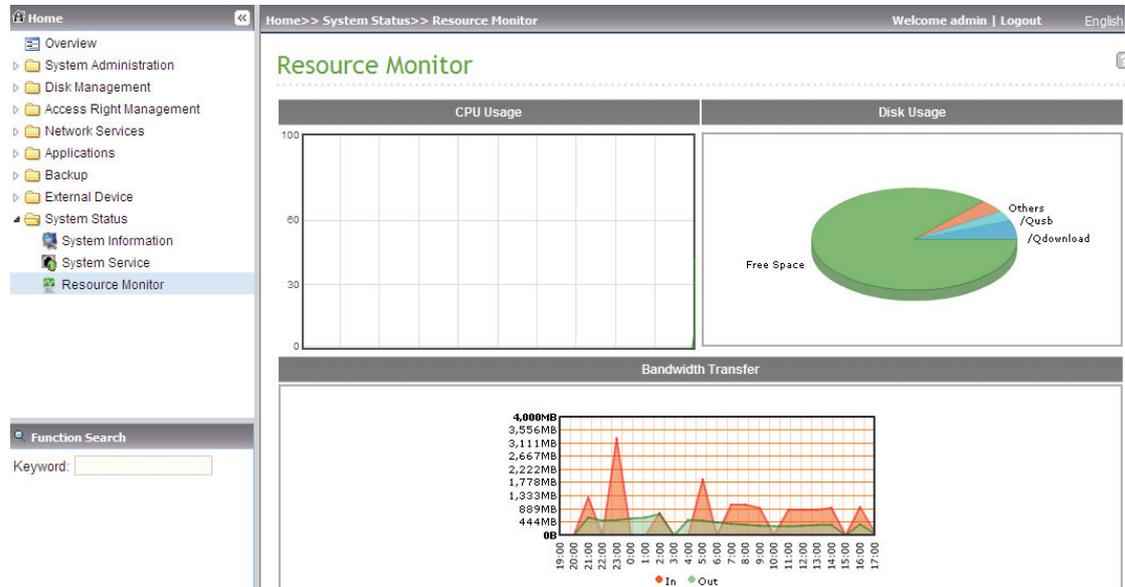
The screenshot displays the 'System Service' configuration page. The left sidebar lists navigation options: Overview, System Administration, Disk Management, Access Right Management, Network Services, Applications, Backup, External Device, System Status (selected), System Information, System Service, and Resource Monitor. Below the sidebar is a 'Function Search' section with a 'Keyword:' input field.

The main content area is titled 'System Service' and contains two columns of service configurations:

System Service	
Microsoft Networking	
Enabled	<input checked="" type="checkbox"/>
Server Type	Standalone Server
Workgroup	NAS
Enable WINS server	<input type="checkbox"/>
Enable Domain Master	<input type="checkbox"/>
Apple Networking	
Enabled	<input checked="" 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
Multimedia Station	
Enable Multimedia Station	<input 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"/>
System Port Management	
Port	8080

3.8.3 Resource Monitor

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

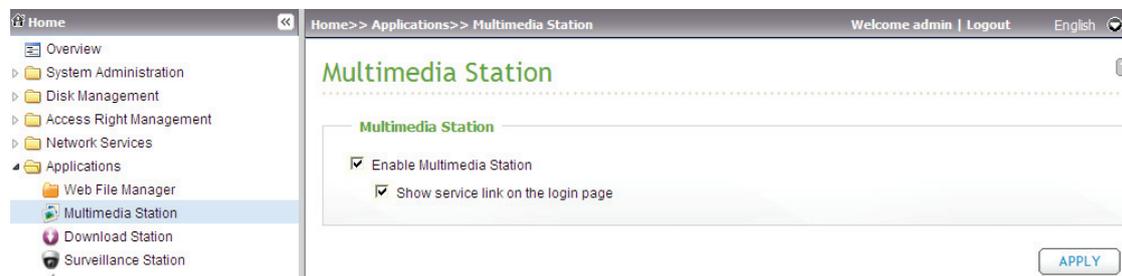


Chapter 4 Multimedia Station

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

Upload photos by web administration

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



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

3. Click 'Login' on the top right hand corner. Login as an administrator. You can create user accounts who are allowed to view the multimedia files.



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



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

Upload the photos to the share folder of the NAS directly

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

1. Open the Windows Run menu. Enter *NAS name* or *NAS IP* to connect to the share folder on the NAS.
2. Open the folder Qmultimedia/ Multimedia. Enter the user name and password to login.
3. Drag the files and folders to the network share folder directly. Please wait patiently when the NAS is generating thumbnails for the images.

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

Buttons on the Multimedia Station page

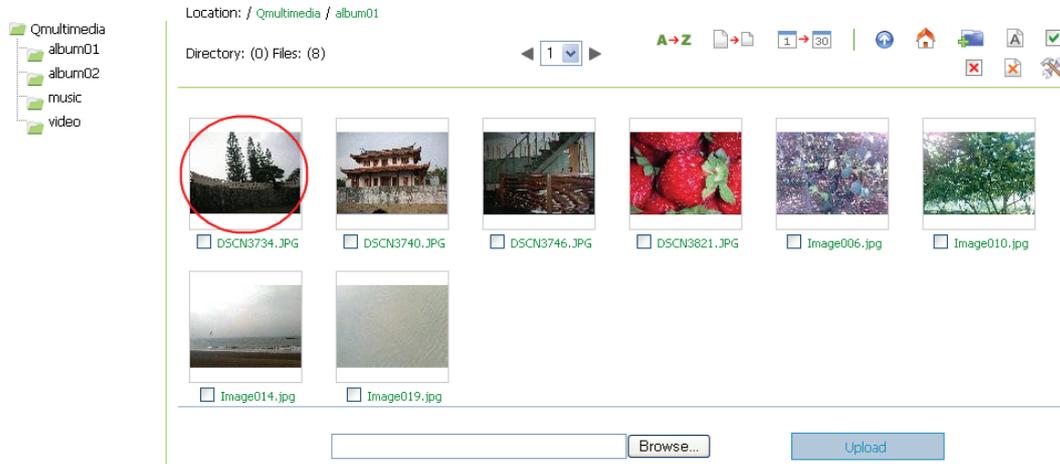
	Sort the files by name
	Sort the files by size
	Sort the files by date
	Return to the previous page
	Return to Home
	Create a folder
	Rename a file or folder
	Select all
	Select none
	Delete

Support file format list

Type	File format
Picture	JPG, BMP, GIF
Video 	WMV, WMX, WVX, AVI, MPEG, MPG, MPE, M1V, MP2, MPV2, MP2V, MPA, DVR-M, ASF, ASX, WPL, WM, WMX, WMD, WMZ
Audio 	WMA, WAX, CDA, WAV, MP3, M3U, MID, MIDI, RMI, AIF, AIFC, AIFF, AU, SND
Others 	(Other formats not mentioned above)

View the photo information

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



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



Buttons description

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

	Return to the previous level
	Previous image
	Next image
	Rotate the image anticlockwise
	Rotate the image clockwise
	Zoom in
	Zoom out
SlideShow: <input type="text" value="3"/>  	Play the slideshow. Select the time interval in seconds. Click 'play' to play the slideshow. To stop playing, click 'stop'.
	Print the image
	Save the picture
	Set the picture as the album cover

Play music or video files

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

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

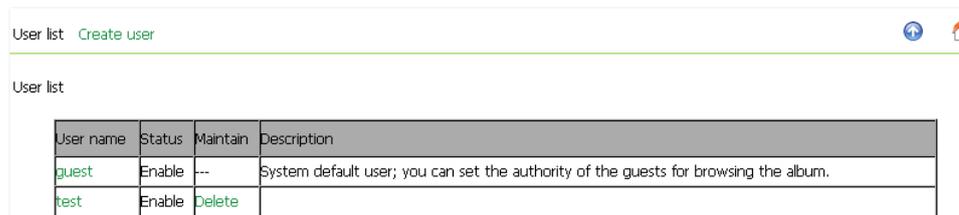


Configure album authority

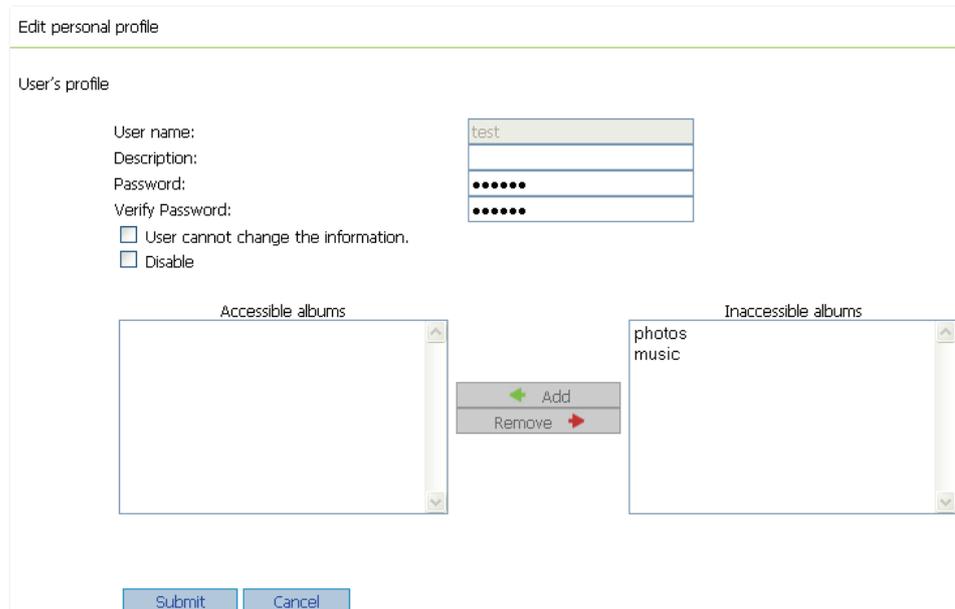
1. After logging in as the administrator (admin), click  to enter the configuration page for album authority.



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



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



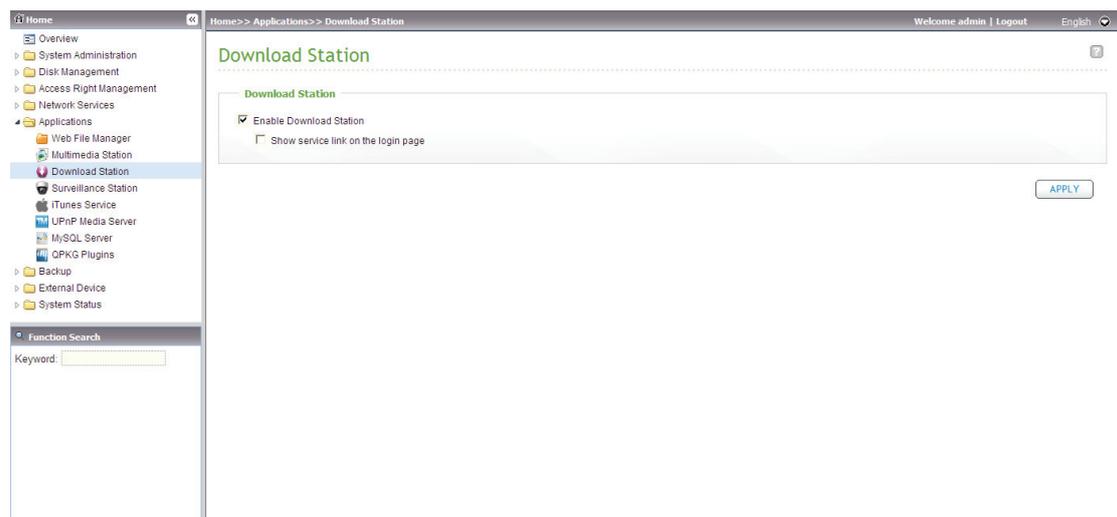
Chapter 5 Download Station

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



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

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

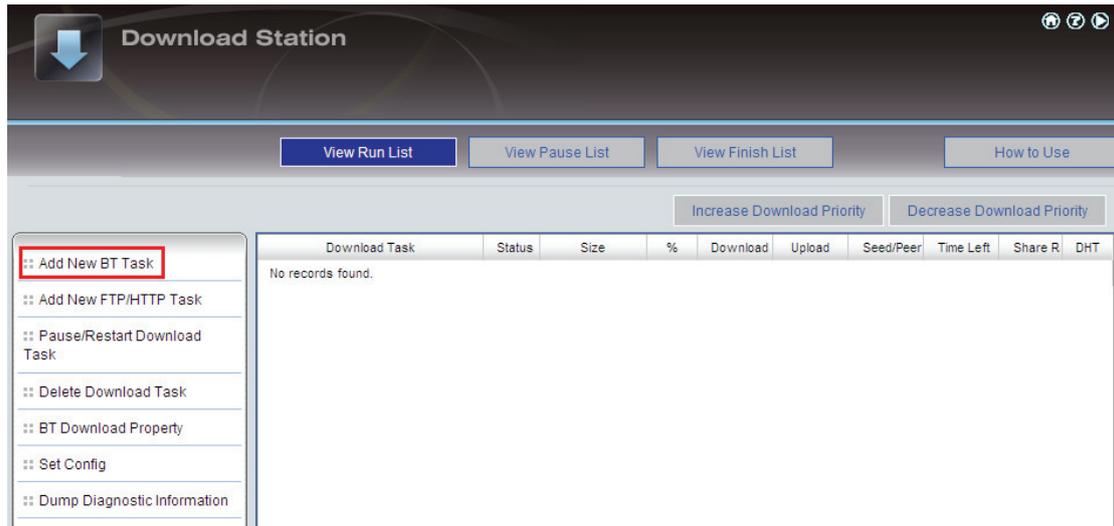


2. Click 'Download Station' on the top or on the login page of the NAS to connect to the Download Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.

3. Select 'Add new BT task' or 'Add new FTP/HTTP task'.

Add a new BT task

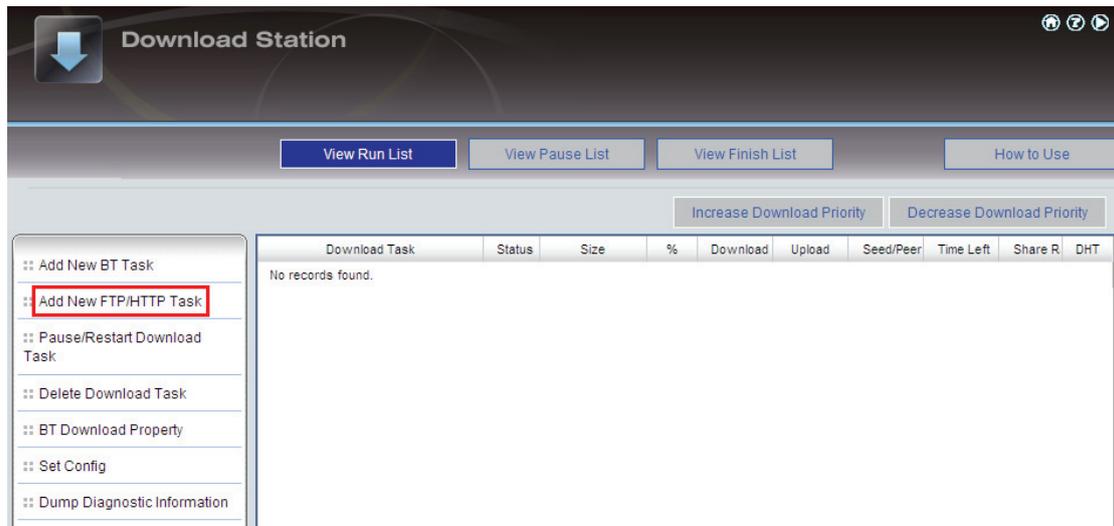
Click 'Add new BT task' on the left and upload a torrent file. You can download the legal torrent files from the Internet. There are websites that provide legally shared torrents, for example www.legaltorrents.com. Please download the torrent files to your local disk and then upload them to the NAS.



Add a new FTP/HTTP task

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

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



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



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

The screenshot shows a software interface with a table of download tasks and a menu on the left. The table has columns for Download Task, Status, Size, %, Download, Upload, Seed/Peer, Time Left, Share R, and DHT. The first row shows a task named 'abc.torrent' with status 'RUN', size '0.00 MB', and 0.0% completion. The left-hand menu includes options like 'Add New BT Task', 'Add New FTP/HTTP Task', 'Pause/Restart Download Task', 'Delete Download Task', 'BT Download Property' (highlighted with a red box), 'Set Config', and 'Dump Diagnostic Information'. At the top right, there are buttons for 'Increase Download Priority' and 'Decrease Download Priority'.

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

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

This screenshot is identical to the one above, showing the same software interface. However, in this version, the 'Set Config' option in the left-hand menu is highlighted with a red box, indicating the next step in the process.

Protocol Encryption

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

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

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



The screenshot shows the Azureus interface. On the left is a sidebar menu with the following options: 'Add New BT Task', 'Add New FTP/HTTP Task', 'Pause/Restart Download Task' (highlighted with a red box), 'Delete Download Task', 'BT Download Property', 'Set Config', and 'Dump Diagnostic Information'. On the right is a table with columns: 'Download Task', 'Status', 'Size', '%', 'Download', 'Upload', 'Seed/Peer', 'Time Left', 'Share R', and 'DHT'. The table contains one row with the following data: 'abc.torrent', 'RUN', '0.00 MB', '0.0', '0.0 KB/s', '0.0 KB/s', '0/0', '99:99:99', 'oo', and 'Off'. Above the table are two buttons: 'Increase Download Priority' and 'Decrease Download Priority'.

Download Task	Status	Size	%	Download	Upload	Seed/Peer	Time Left	Share R	DHT
abc.torrent	RUN	0.00 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	99:99:99	oo	Off

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

The screenshot shows the Download Station interface. At the top right, there are two buttons: "Increase Download Priority" and "Decrease Download Priority", both highlighted with a red border. Below these buttons is a table with the following data:

Download Task	Status	Size	%	Download	Upload	Seed/Peer	Time Left	Share R	DHT
abc.torrent	RUN	0.00 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	99:99:99	oo	Off
cde.torrent	RUN	0.00 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	99:99:99	oo	Off

On the left side of the interface, there is a menu with the following options:

- :: Add New BT Task
- :: Add New FTP/HTTP Task
- :: Pause/Restart Download Task
- :: Delete Download Task
- :: BT Download Property
- :: Set Config
- :: Dump Diagnostic Information

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

This screenshot is similar to the previous one, but the "Delete Download Task" button in the left-hand menu is highlighted with a red border. The table and buttons at the top right remain the same as in the previous screenshot.

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

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

Dump Diagnostic Information

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

The screenshot shows the main interface of the Download Station. At the top right, there are two buttons: 'Increase Download Priority' and 'Decrease Download Priority'. Below them is a table with columns: Download Task, Status, Size, %, Download, Upload, Seed/Peer, Time Left, Share R, and DHT. The table contains two rows: 'abc.torrent' and 'cde.torrent', both with a status of 'RUN' and 0.0 MB size. On the left side, there is a sidebar with several options, each preceded by '::'. The option 'Dump Diagnostic Information' is highlighted with a red rectangular border.

The screenshot shows a dialog box titled 'Download Station'. The main content area is titled 'Dump Diagnostic Information:' and displays the following details for the selected task:

- Download Task: cde.torrent
- Size: 0.00 MB
- Percent: 0.0 %
- Download Totals: 0.0 MB
- Upload Total: 0.0 MB
- Share Time: 0 hr
- Start Time: Tue Apr 20 17:26:00 2010

At the bottom left, it says 'No Error!'. At the bottom right, there is an 'OK' button.

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

The screenshot shows the same interface as the previous one, but with a right-click context menu open over the 'cde.torrent' task in the table. The menu items are: 'Increase Download Priority', 'Decrease Download Priority', 'Pause/Restart Download Task', 'Delete Download Task', 'BT Download Property', and 'Dump Diagnostic Information'.

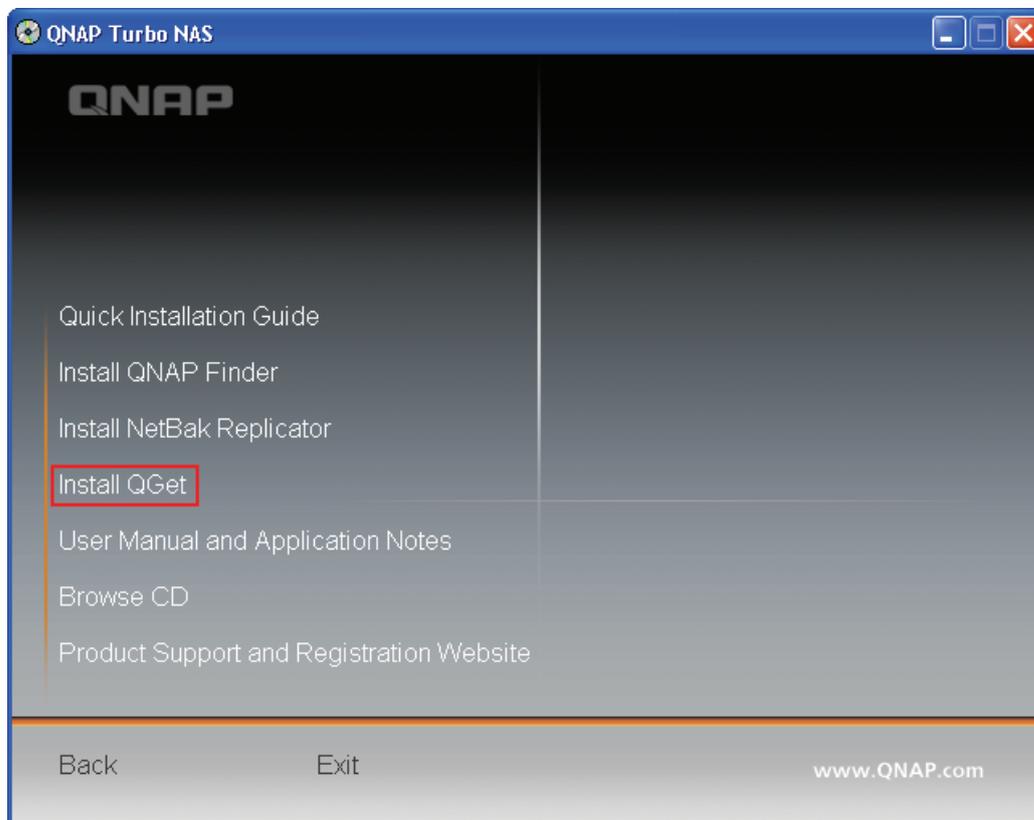
The common reasons for slow BT download rate or download error are as below:

- (1) The torrent file has expired, the peers have stopped sharing this file, or there is an error in the file.
- (2) The NAS has configured to use fixed IP but DNS server is not configured, or DNS server fails.
- (3) Set the maximum number of simultaneous downloads as 3-5 for the best download rate.
- (4) The NAS is located behind NAT router. The port settings have led to slow BT download rate or no response. You may try the following means to solve the problem:
 - a. Open the BitTorrent port range on NAT router manually. Forward these ports to the LAN IP of the NAS.
 - b. The new NAS firmware supports UPnP NAT port forwarding. If your NAT router supports UPnP, enable this function on the NAT. Then enable UPnP NAT port forwarding of the NAS. The BT download rate should be enhanced.

5.1 Use Download Software QGet

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

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



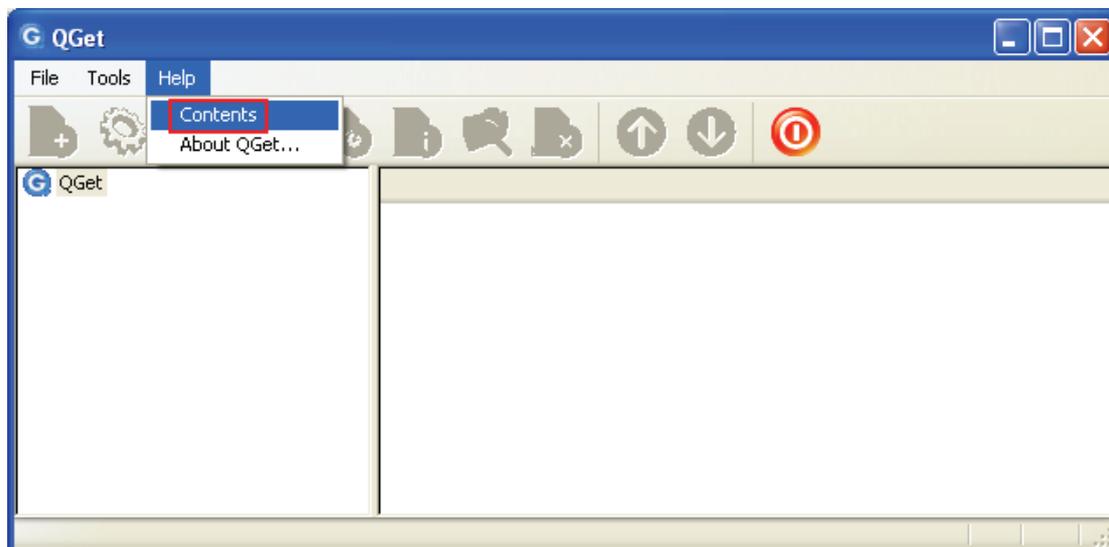
2. Follow the instructions to install QGet.



3. Run QGet from the installed location.



4. For the details of using QGet, see the online help.



Chapter 6 Web File Manager

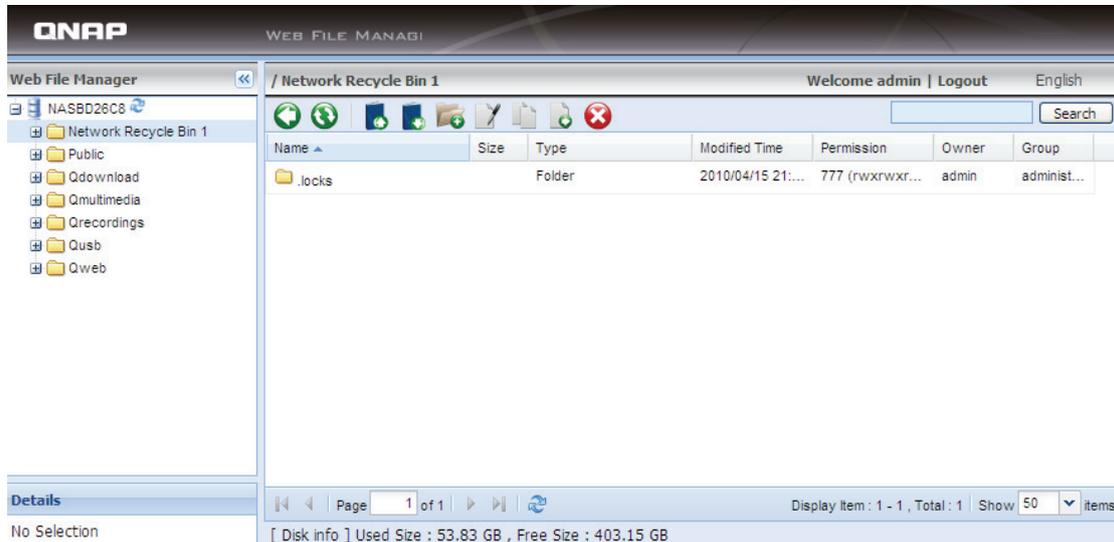
To use Web File Manager, go to 'Applications' > 'Web File Manager'. Enable the service.



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

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

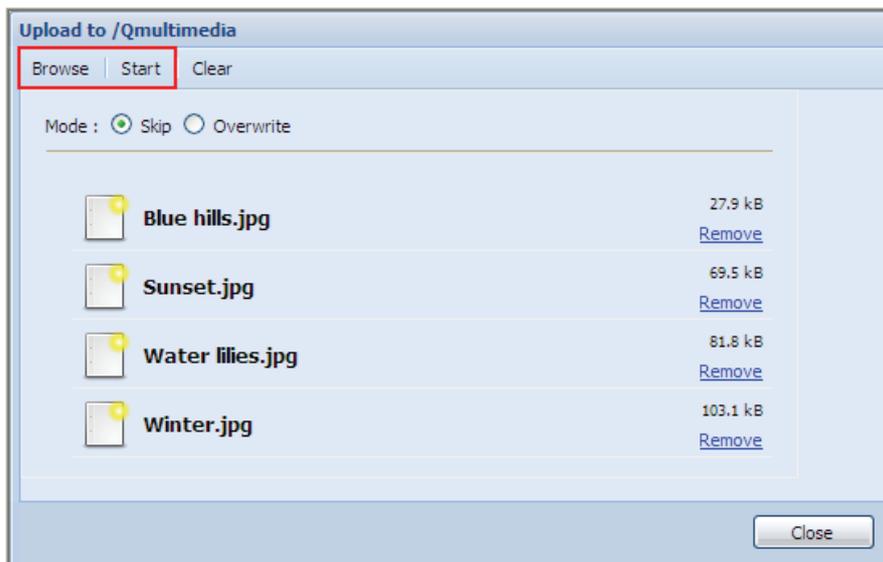
You can organize the network share folders of the NAS. With Web File Manager, you can upload, download, rename, move, copy, or delete the files and folders in the network shares.



Upload file

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

- i. Open the folder to upload file to. Click .
- ii. Click 'Browse' to select the file(s).
- iii. Select to skip or overwrite the existing file in the folder.



- iv. Click 'Start'.

Download file

- i. Select a file or folder to download.
- ii. Right click the mouse and select 'Download' or click  to download the file.

Create folder

- i. Select a network share or folder in which you want to create a new folder.
- ii. Click  (Create Folder).
- iii. Enter the name of the new folder and click 'OK'.

Rename file or folder

- i. Select a file or folder to rename.
- ii. Click  (Rename).
- iii. Enter the new file or folder name and click 'OK'.

Copy files or folders

- i. Select the files or folders to copy.
- ii. Click  (Copy).
- iii. Select the destination folder.
- iv. Select to skip or overwrite the existing file in the destination folder. Click 'OK'.

Move files or folders

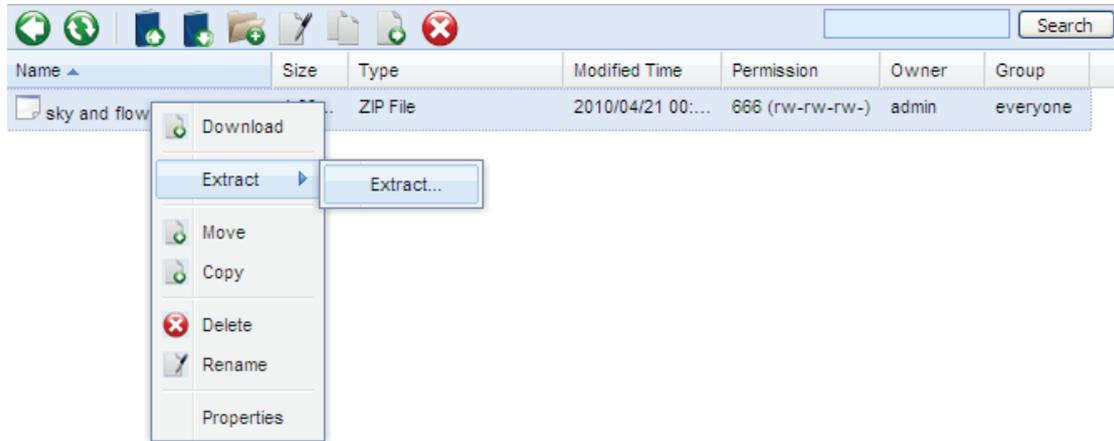
- i. Select the files or folders to move.
- ii. Click  (Move).
- iii. Select the destination folder.
- iv. Select to skip or overwrite the existing file in the destination folder. Click 'OK'.

Delete file or folder

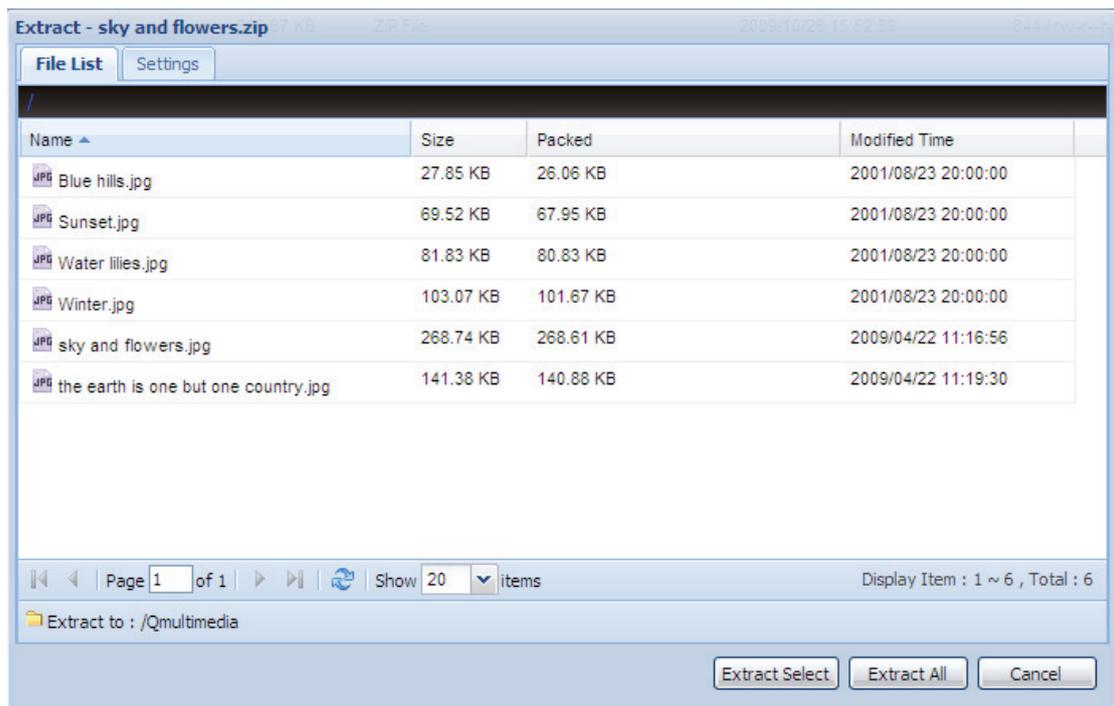
- i. Select a file or folder to delete.
- ii. Click  (Delete) on the toolbar.
- iii. Confirm to delete the file or folder.

Extract files

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



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



Chapter 7 NetBak Replicator

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

Main Functions

1. Backup

- **Instant Backup**
Select the files and folders on the local PC and back up the files to the network share folders on the NAS immediately.
- **File Filter**
Select particular file types to be excluded from backup. The NAS will filter all the specified file types when backing up the data.
- **Schedule**
Specify a schedule for backing up the data, for example, 12:00 every day or 05:00 every Saturday.
- **Monitor**
When this option is enabled, the system will upload all the files or folders to the server instantly for backup when the files or folders are modified.

2. Restore

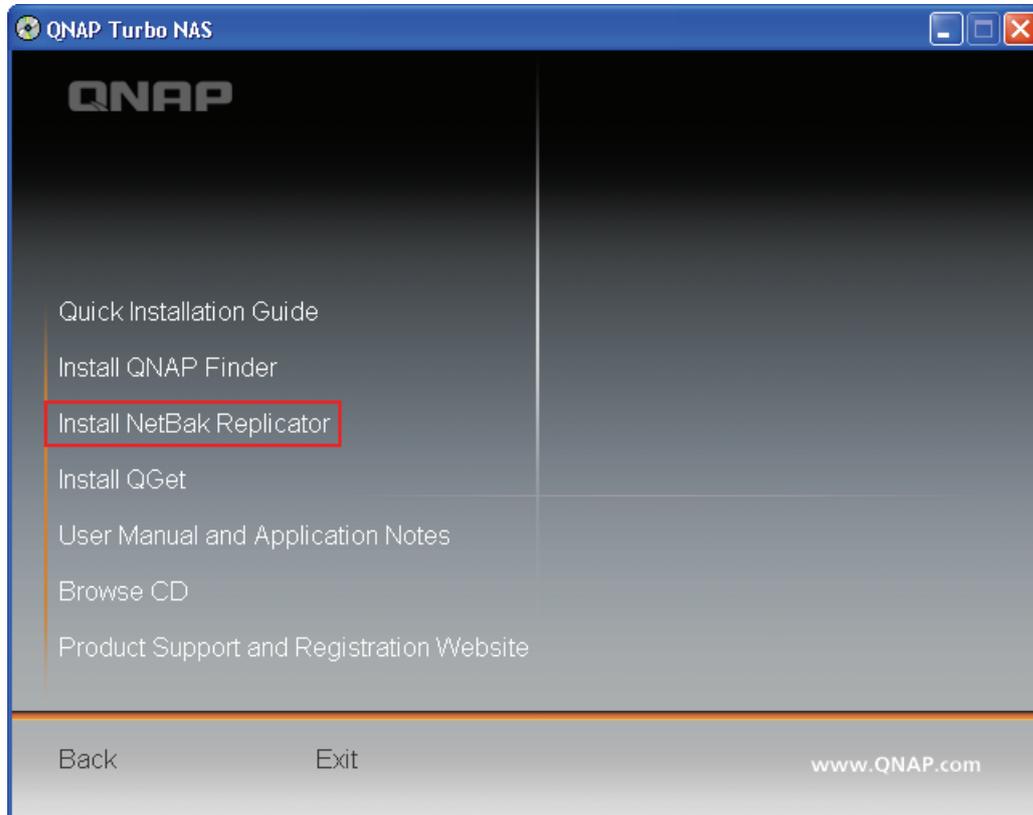
Select this option to restore the backup data to the original location of the file or to a new directory.

3. Log

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

Install NetBak Replicator

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



2. Follow the instructions to install NetBak Replicator.

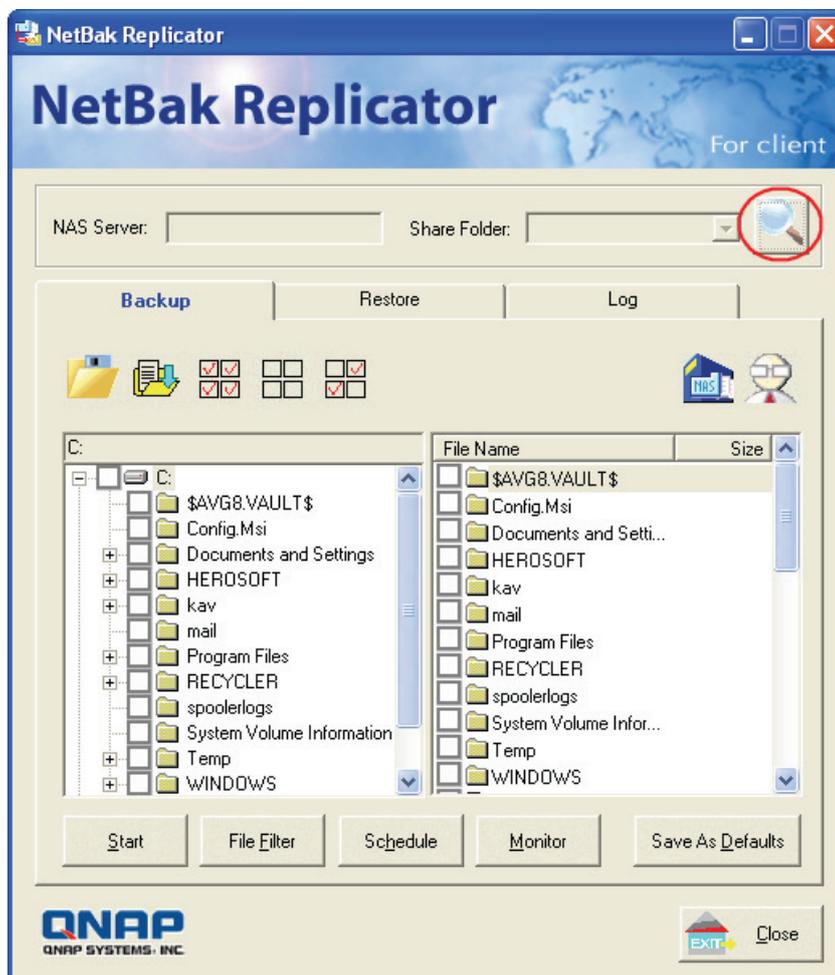


3. Upon successful installation, a shortcut icon  will be shown on the Desktop. Double click the icon to run NetBak Replicator.

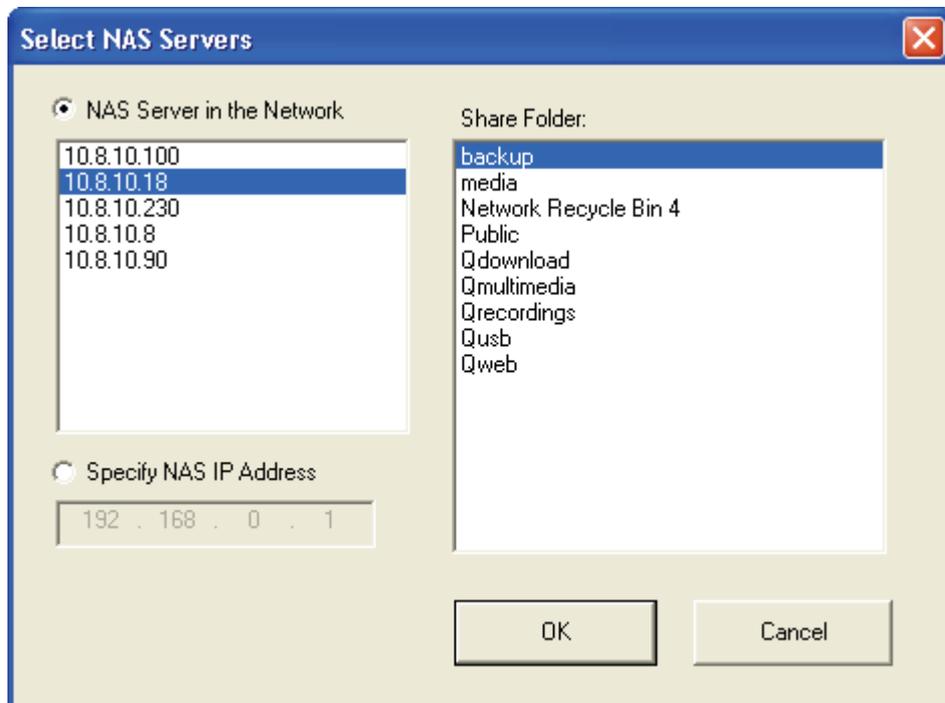
Use NetBak Replicator

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

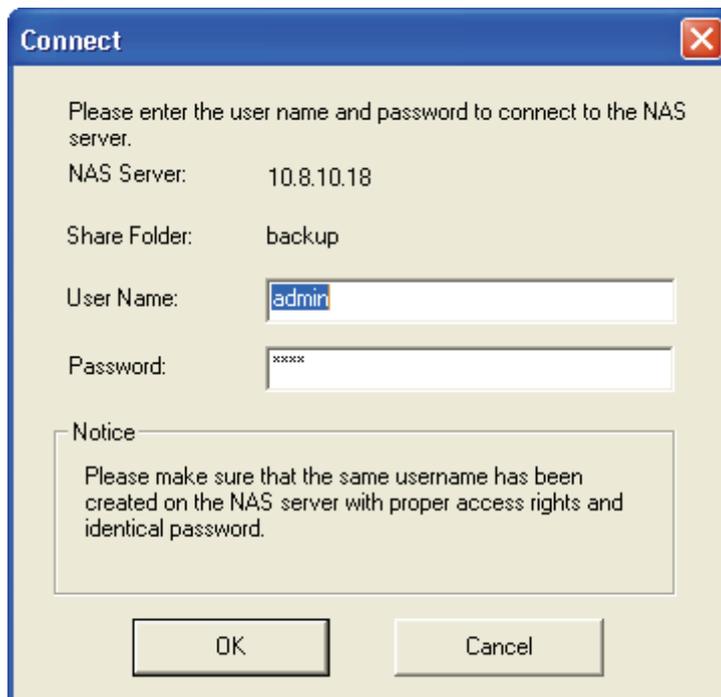
2. Run NetBak Replicator. Click . All the NAS on the local network and their share folders will be displayed.



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



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



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

Description of the buttons on NetBak Replicator

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

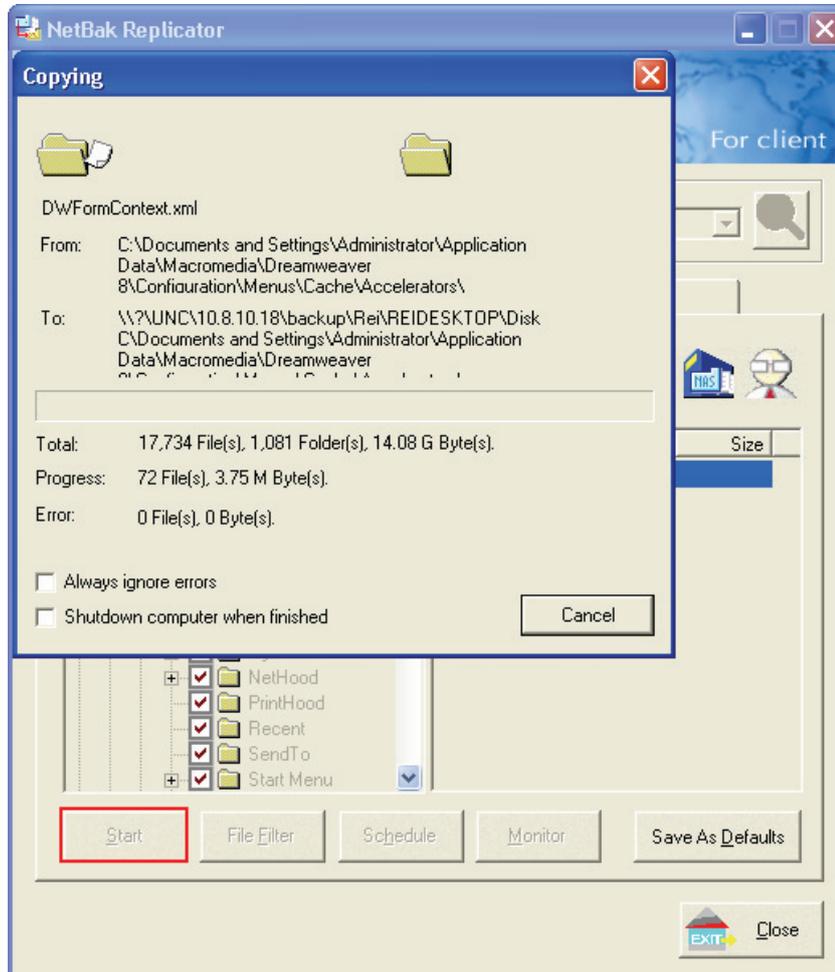
- **Backup**

Select the files and folders for backup.



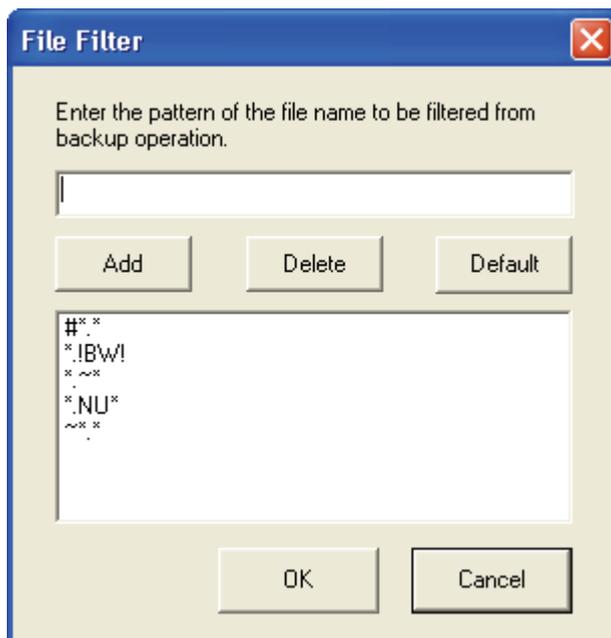
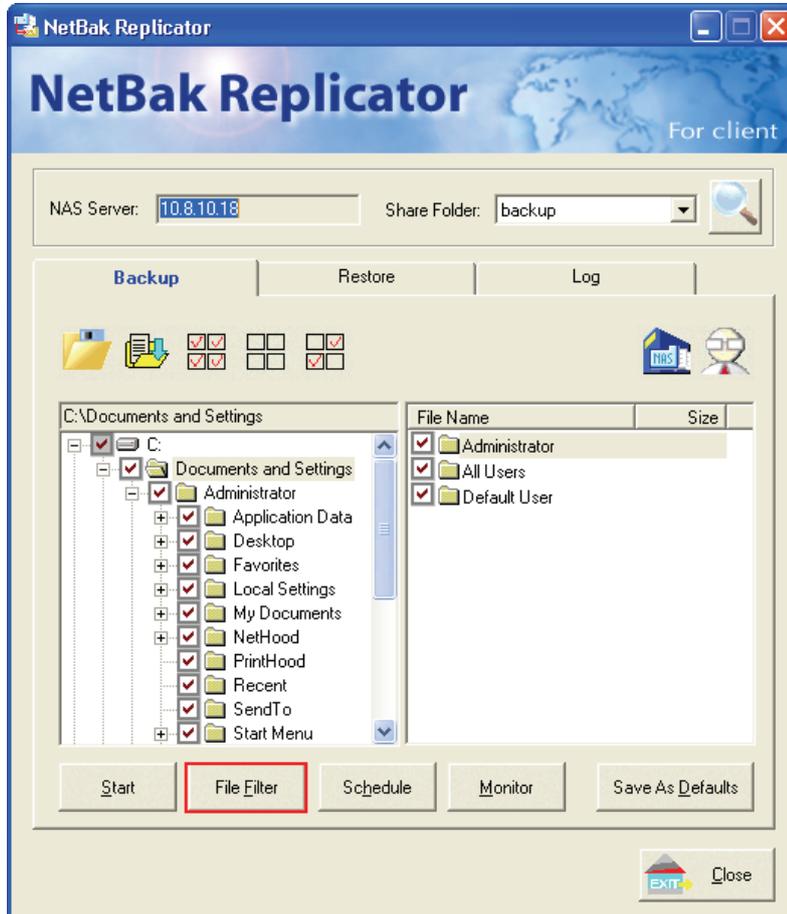
✓ Start

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



✓ File Filter

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



✓ Schedule

Click 'Schedule' on the main page of NetBak Replicator. Then select the option 'Enable Backup Schedule' and select the frequency and time for backup. Click 'OK' to confirm.



Backup Schedule ✖

Select the frequency and time for backup.

Enable Backup Schedule

Start Time:

Frequency

Back up everyday.

Back up on selected week day(s).

Sunday Monday Tuesday Wednesday

Thursday Friday Saturday

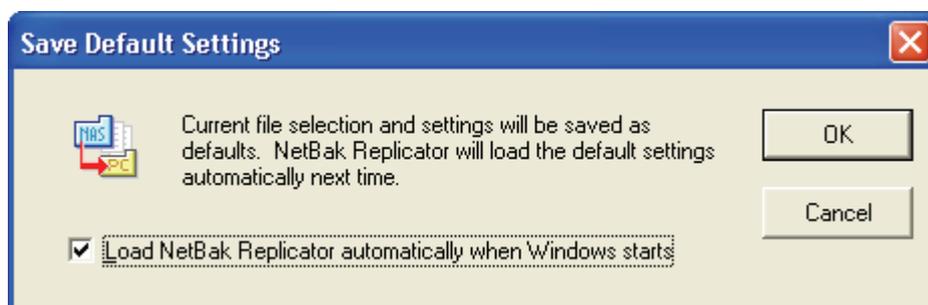
✓ Monitor

Select a folder for monitoring. When this option is enabled, all the new and modified files on the PC will be copied to the NAS instantly. Other files will be gray and cannot be selected. Click 'Monitor' again to stop monitoring. An icon  will appear on task bar of Windows when monitoring is in process.



✓ Save as Defaults

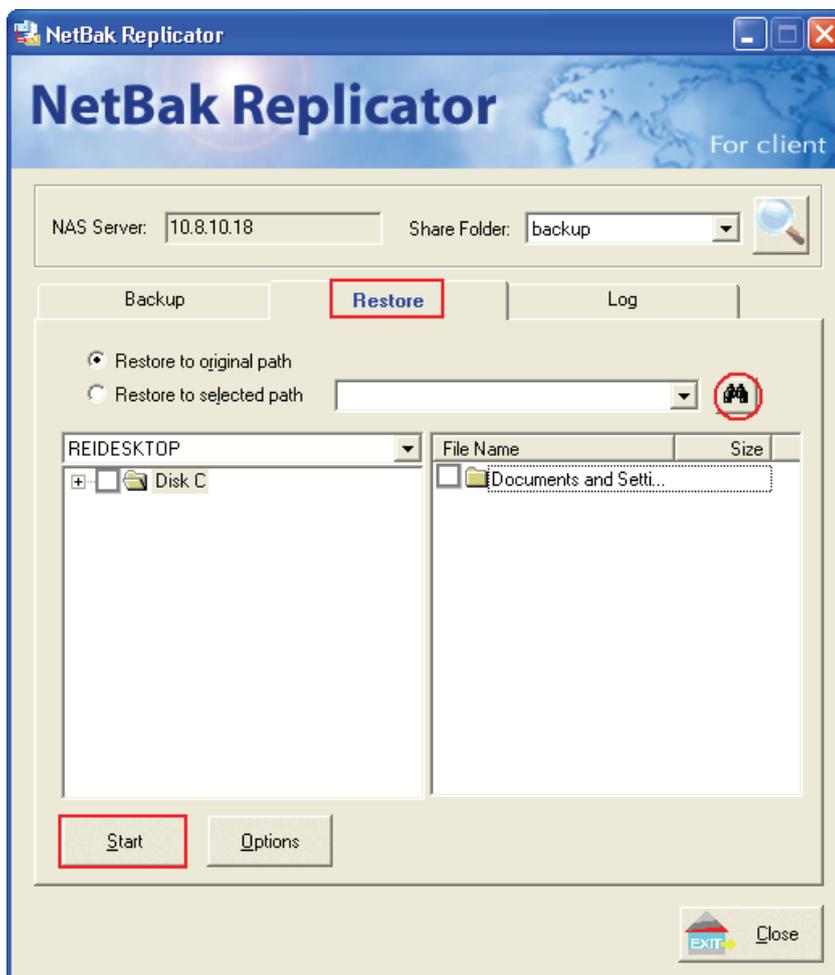
Click this button to save the current settings of NetBak Replicator as the defaults. When you login again, the program will load the default settings automatically. You can also select to load the utility automatically when Windows starts.



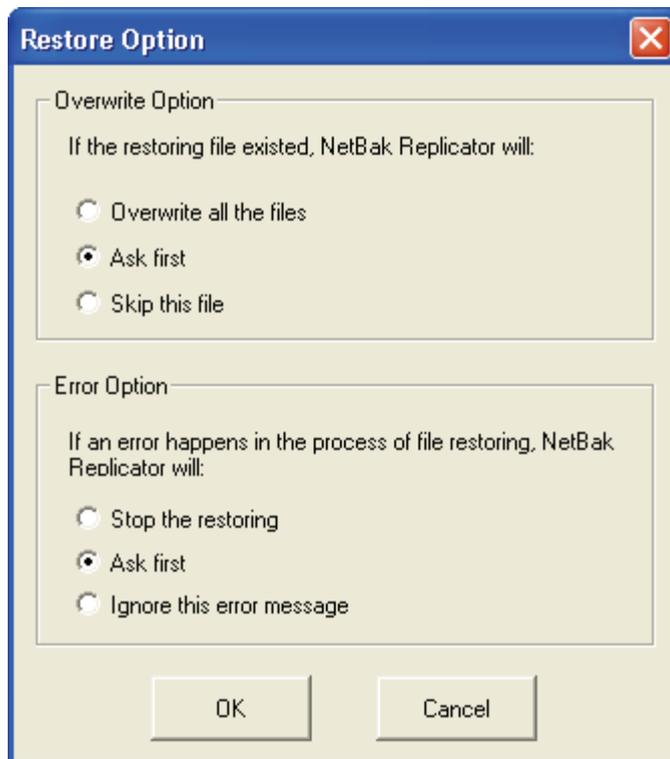
- **Restore**

Follow the steps below to restore the files from the NAS to your PC.

- a. Click  to select the NAS and the share folder (the restore source).
- b. Click the 'Restore' tab on NetBak Replicator.
- c. Select to restore the data to the original path or click  to specify the restore location manually.
- d. Select the files and folders to restore.
- e. Click 'Start'.



- f. Options: Select the behaviour of NetBak Replicator if the restored file exists on the destination and when an error occurs during the process.



- **Log**

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



Chapter 8 Active Directory

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

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

Join the QNAP NAS to Microsoft Active Directory

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 a web-based configuration interface. On the left is a navigation menu with categories like System Administration, Hardware, Security, and Network Services. The 'Network' option is selected. The main content area is titled 'Home >> System Administration >> Network'. At the top, it says 'Use the settings from: Ethernet 1+2'. Below this is a section for 'Port Trunking' with a checked checkbox 'Enable Network Port Trunking' and a dropdown menu set to 'Active Backup(Fail Over)'. The 'DNS Server:' section is highlighted with a red box and contains two rows of IP address input fields: 'Primary DNS Server: 10 . 8 . 2 . 11' and 'Secondary DNS Server: 10 . 8 . 2 . 9'.

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

Home >> Network Services >> Microsoft Networking

Microsoft Networking

MICROSOFT NETWORKING **ADVANCED OPTIONS**

Microsoft Networking

Enable file service for Microsoft networking

Standalone Server

Server Description (Optional):

Workgroup:

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

Server Description (Optional):

Domain NetBIOS Name:

AD Server Name:

Domain:

Organization Unit (Optional):

Domain Administrator Username:

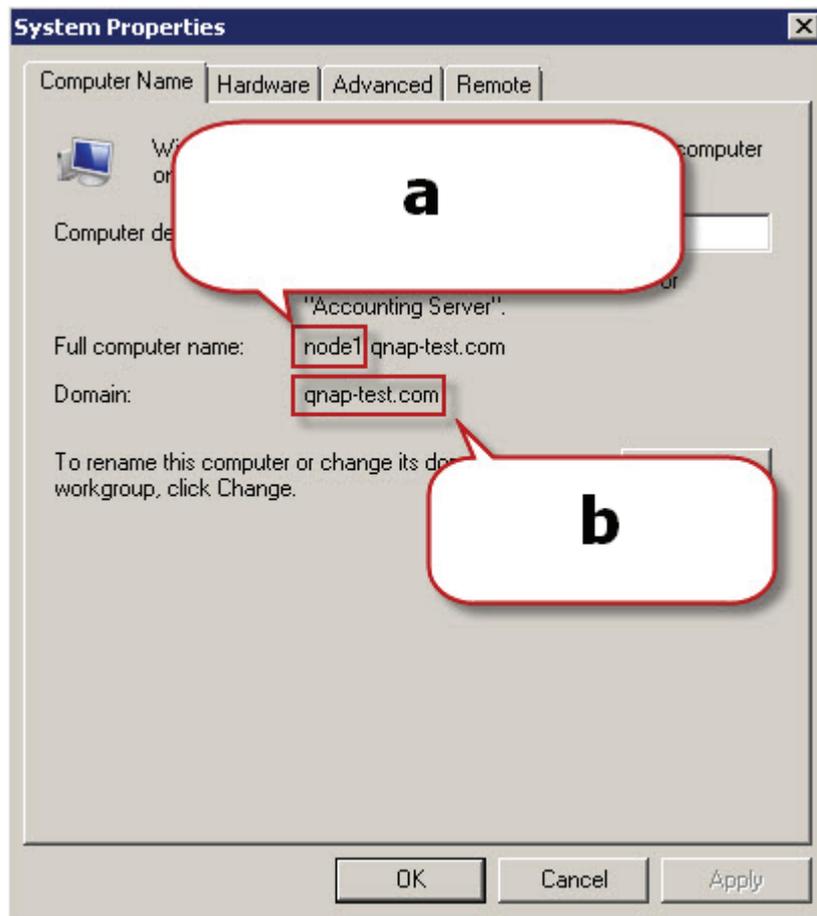
Domain Administrator Password:

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.
- The domain administrator password must not contain the special symbol '!', or the NAS will fail to join the AD domain.

Windows 2003:

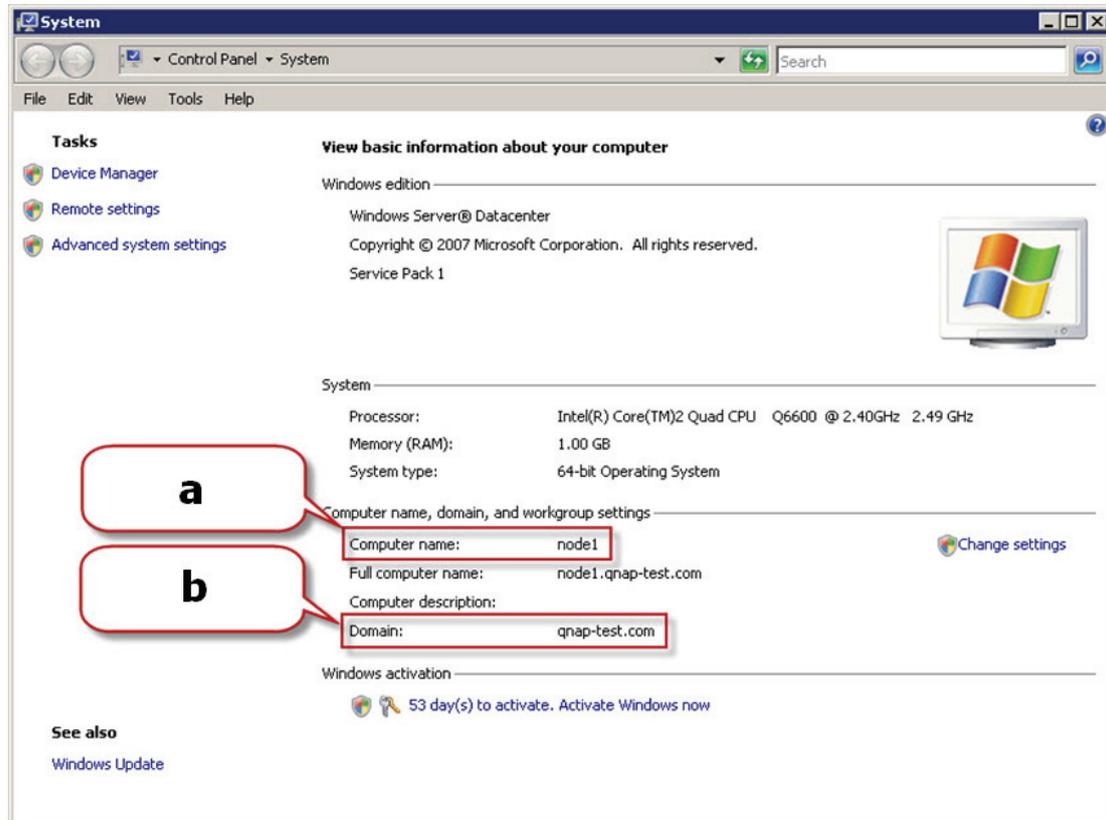
You may check the AD server name and AD domain name in 'System Properties'.



- 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:

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



- a. This is your AD server name.
- b. This is your domain name.

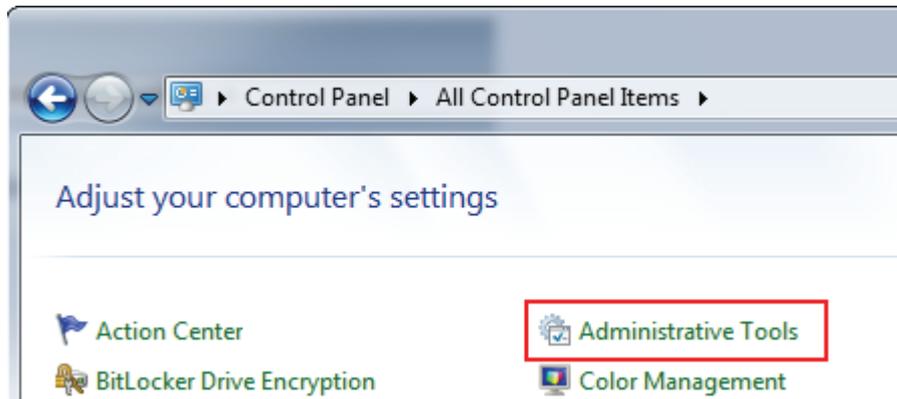
Notes:

- After joining the NAS to the Active Directory, the local NAS users who have access right to the AD server should use '**NASname\username**' to login; the AD users should use their own user names to login the AD server.
- The local NAS users and the AD users (with username as domain name + username) are allowed to login the NAS (firmware version 3.2.0 and above) via AFP, FTP, Web File Manager, and WebDAV. However, if the firmware version of the NAS is earlier than 3.2.0, only 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 later.

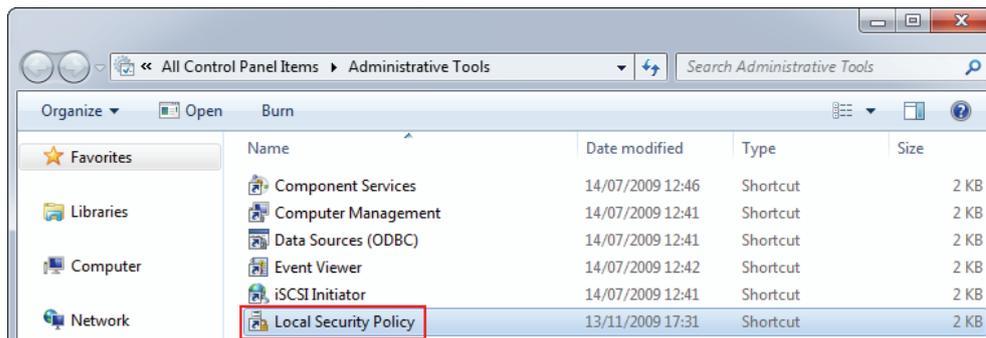
Windows 7:

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.

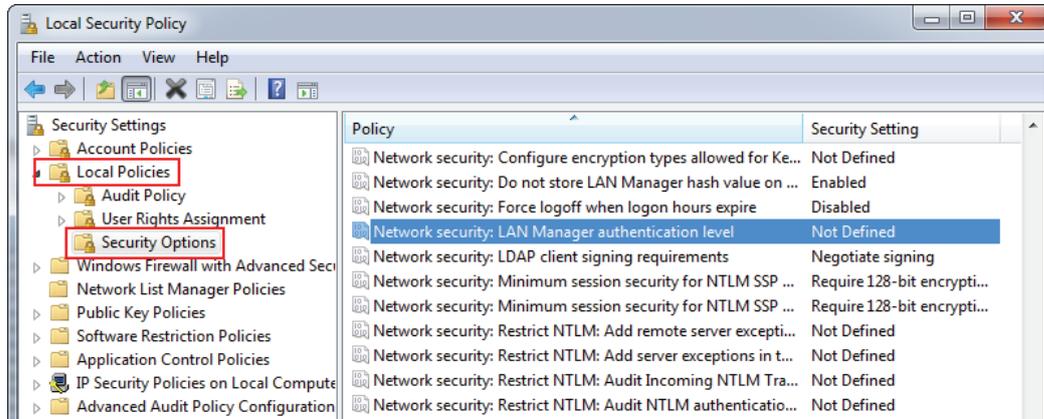
(a) Go to the 'Control Panel', and click 'Administrative Tools'.



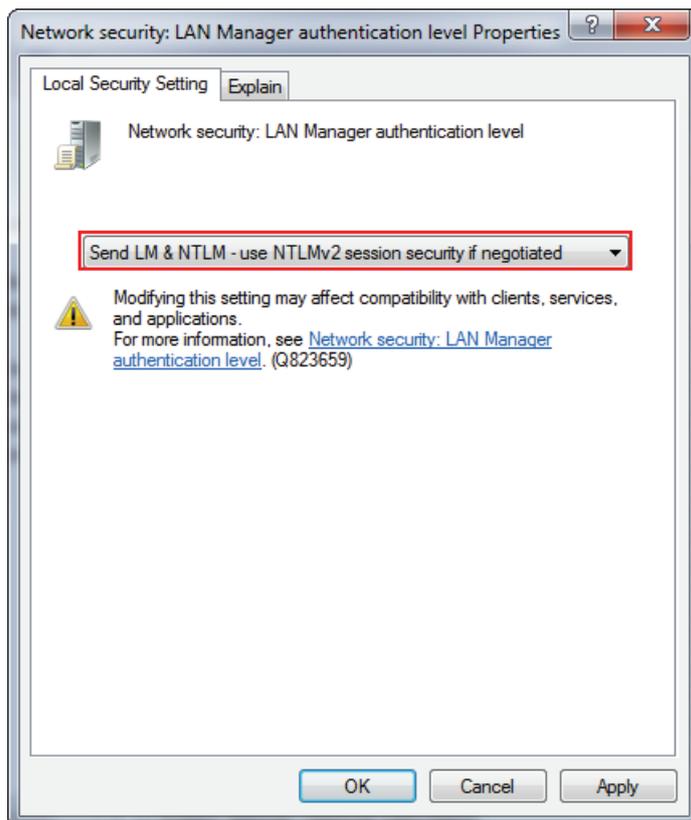
(b) Click 'Local Security Policy'.



- (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 & NTLM – use NTLMv2 session security if negotiated' from the list. Then click 'OK'.



Chapter 9 NAS Maintenance

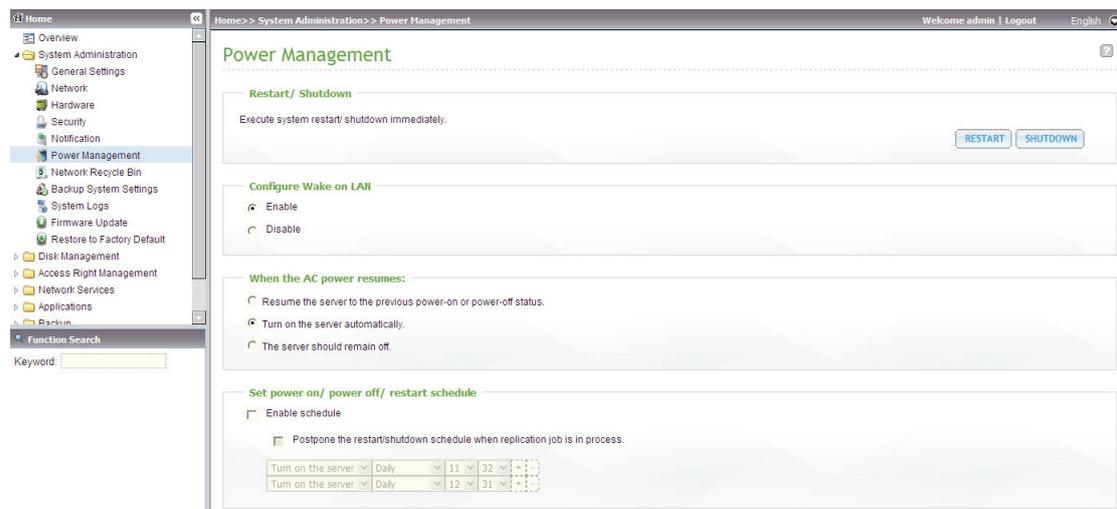
9.1 Restart/ Shut down Server

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

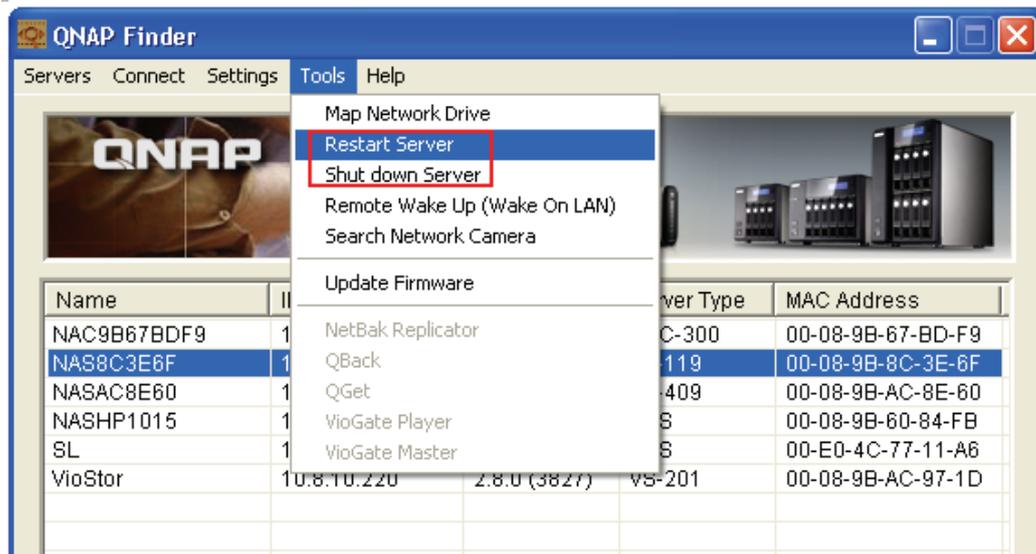
1. Login the NAS as an administrator. Go to 'System Administration' > 'Power Management'.
2. Click 'Restart' to reboot the server or 'Shut Down' to turn off the server.

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

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

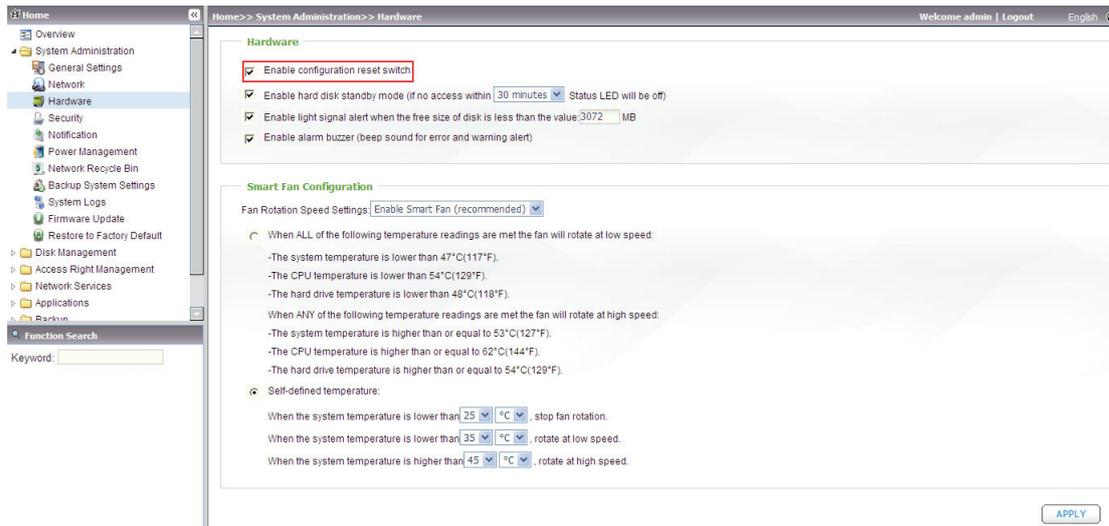


You can use the Finder to restart or shut down the server. You must have an administrator account to perform this action.



9.2 Reset Administrator Password and Network Settings

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



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

Basic system reset (3 sec)

When you press the reset button for 3 seconds, a beep sound will be heard. The following settings 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)*

*This feature is only provided by TS-439 Pro, TS-439 Pro II, TS-459 Pro, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, and TS-809U-RP.

Advanced system reset (10 sec)

When you press the reset button for 10 seconds, you will hear two beeps at the third and the tenth seconds. The NAS will reset all the system settings to default as it does by 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 share folders you previously created will be cleared. To retrieve the old data after the advanced system reset, you may create the same network share folders on the NAS and the data will be accessible again.

9.3 Disk Failure or Malfunction

When you encounter HDD malfunction or failure, do the following:

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



Caution:

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

9.4 Power Outage or Abnormal Shutdown

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

1. If the system configuration is lost, configure the NAS again.
2. In the NAS does not function properly and re-configuration does not work, contact the technical support.

9.5 System Software Abnormal Operation

When the system software does not operate properly, the NAS automatically restarts to resume normal operation. If you find the NAS restarts repetitively, contact the technical support immediately.

9.6 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 HDD temperature exceeds 65°C (149°F)*

* Note that when the temperature of any HDD 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 HDD exceeds 65°C (149°F) continuously after 15 (5+10) minutes.

Chapter 10 RAID Operation Troubleshooting

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

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

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

2. Find out the HDD that causes the RAID rebuilding failure.

You can go to 'System Administration' > 'System Logs' page to search for the following error message and find out which HDD causes the error.

Error occurred while accessing Drive **X**.

Drive **X** has been removed.

X refers to the number of the hard drive slot.

3. Troubleshooting

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

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

If the newly plugged in HDD (for example, HDD 1) causes the rebuilding error, please unplug HDD 1 and plug in another new HDD to start RAID rebuilding.

Situation 2: The error is caused by an existing HDD (for example, HDD 2) in the RAID configuration.

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

- a. Back up the HDD data to another storage device. Then reinstall and set up the NAS.
- b. Format the newly plugged in HDD (for example, HDD 1) as a single drive. Then back up the data on the NAS to this drive (HDD 1) via Web File Manager. Unplug the HDD with errors (for example, HDD 2). After that, insert a new HDD to NAS to replace the fault drive, and execute RAID 1 migration.

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



Caution: When plugging in or unplugging a HDD, please strictly adhere to the following rules to avoid abnormal system operation or data damage.

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

Chapter 11 Use the LCD Panel

This feature is only provided by TS-439 Pro, TS-439 Pro II, TS-459 Pro, TS-509 Pro, TS-639 Pro, TS-659 Pro, SS-839 Pro, TS-859 Pro, TS-809 Pro, and TS-809U-RP.

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 server 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 HDD detected and the IP address. You may select to configure the HDD.

Number of HDD 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 HDD 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 HDD, 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 share folders and upload files to the folders on the NAS. In the meantime, to make sure the stripes and blocks in all the RAID component devices are ready, the NAS will execute RAID synchronization and the progress will be shown on 'Disk Management' > 'Volume Management' page. The synchronization rate is around 30-60 MB/s (vary by HDD models, system resource usage, etc.).

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

To encrypt the disk volume*, select 'Yes' when the LCD panel shows <Encrypt Volume?>. The default encryption password is 'admin'. To change the password, 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 server 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, and TS-419U.

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 server name and IP address, you may press the 'Enter' button to enter the Main Menu. The Main Menu consists of the following items:

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

1. TCP/ IP

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

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

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

2. Physical disk

In Physical disk, you can view the following options:

- 2.1 Disk Info
- 2.2 Back to Main Menu

The disk info shows the temperature and the capacity of the HDD.

D	i	s	k	:	1		T	e	m	p	:	5	0	°	C
S	i	z	e	:		2	3	2		G	B				

3. Volume

This section shows the HDD 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

4. 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		

5. Shut down

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

6. Reboot

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

7. Password

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

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

8. Back

Select this option to return to the main menu.

System Messages

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

S y s t e m E r r o r !
P l s . C h e c k L o g s

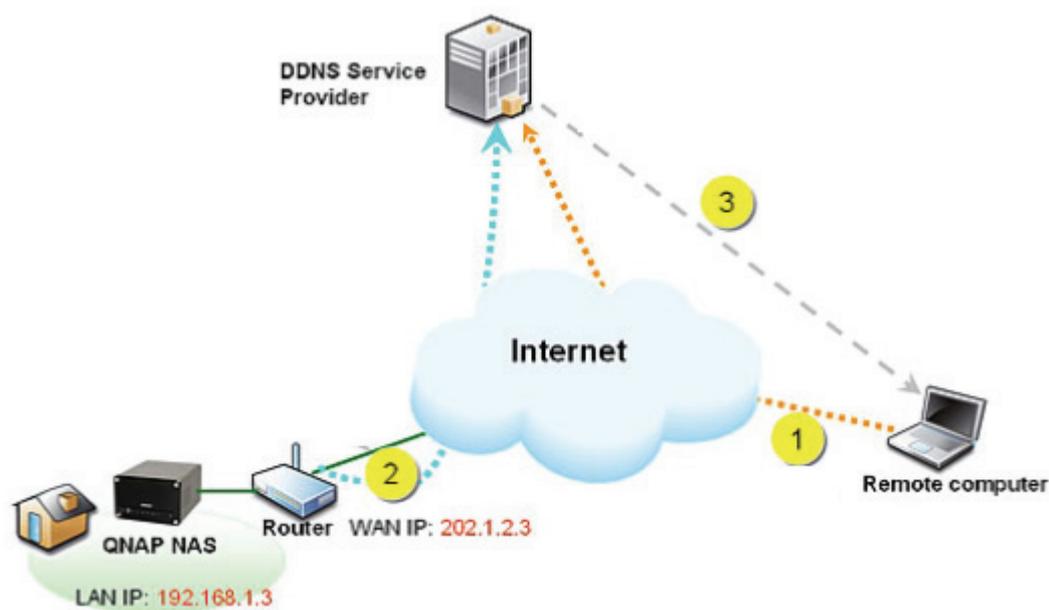
System Message	Description
Sys. Fan Failed	The system fan failed
Sys. Overheat	The system overheat
HDD Overheat	The HDD overheat
CPU Overheat	The CPU overheat
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-balancing mode
LAN1 Lost	LAN 1 is disconnected
LAN2 Lost	LAN 2 is disconnected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

Appendix A. Connect to QNAP NAS from the Internet

Register DDNS and set port forwarding on the NAS

To connect to your NAS at home or office from the Internet, you can enter the IP address of the NAS in a web browser providing that a fixed public IP is assigned to the NAS. However, most users may have installed their NAS behind a NAT router and they are using a dynamic IP for Internet connection. It is inconvenient to memorize an IP address such as 202.193.126.45 and to inform every user of the IP address whenever a new one is assigned by the ISP. You can register a free DDNS account and set up the information on your NAS so that the users can connect to the NAS with an easy-to-remember host name that you specify.

DDNS usage scenario



1. The user connects to the NAS by the URL **<http://qnapqnap.dyndns.org>**.
2. The NAS detects the WAN IP has changed and the DDNS client sends the WAN IP to the DDNS service provider.
3. The DDNS service provider receives the information and assigns the new IP to the DDNS host name (qnapqnap.dyndns.org).

Register a free DDNS account

To register a DDNS account, refer to the steps below. We will be using the DDNS service provided by DynDNS (<http://www.dyndns.com/>) in this example. QNAP NAS currently supports the following DDNS providers:

<http://www.dyndns.com/>

<http://update.ods.org/>

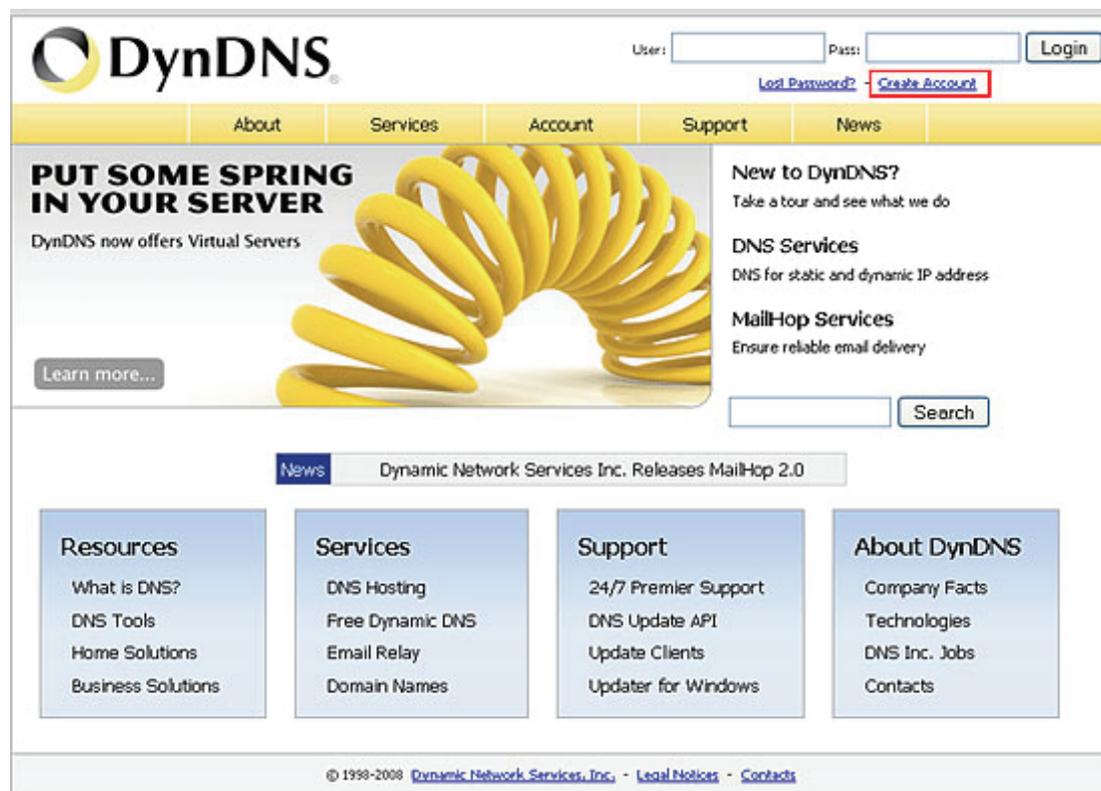
<http://www.dhs.org/>

<http://www.dyns.cx/>

<http://www.3322.org/>

<http://www.no-ip.com/>

Visit <http://www.dyndns.com/> and click 'Create Account' to register an account.



The screenshot shows the DynDNS website homepage. At the top left is the DynDNS logo. To the right are login fields for 'User:' and 'Pass:' with a 'Login' button. Below these is a 'Lost Password?' link and a 'Create Account' button highlighted with a red box. A yellow navigation bar contains links for 'About', 'Services', 'Account', 'Support', and 'News'. The main content area features a large yellow coiled spring graphic with the text 'PUT SOME SPRING IN YOUR SERVER' and 'DynDNS now offers Virtual Servers'. To the right of the spring is a 'Learn more...' button. Further right are sections for 'New to DynDNS?' (with a 'Take a tour and see what we do' link), 'DNS Services' (for static and dynamic IP address), and 'MailHop Services' (to ensure reliable email delivery). Below these is a search bar with a 'Search' button. A 'News' section highlights 'Dynamic Network Services Inc. Releases MailHop 2.0'. At the bottom, there are four columns of links: 'Resources' (What is DNS?, DNS Tools, Home Solutions, Business Solutions), 'Services' (DNS Hosting, Free Dynamic DNS, Email Relay, Domain Names), 'Support' (24/7 Premier Support, DNS Update API, Update Clients, Updater for Windows), and 'About DynDNS' (Company Facts, Technologies, DNS Inc. Jobs, Contacts). The footer contains copyright information: '© 1998-2008 Dynamic Network Services, Inc. - Legal Notices - Contacts'.

Complete the form to create your free account.

Create Your DynDNS Account

Please complete the form to create your free DynDNS Account.

User Information

Username:	<input type="text" value="qnappqnap"/>	
Email Address:	<input type="text" value="██████@qnapp.com"/>	Instructions to activate your account will be sent to the email address provided.
Confirm Email Address:	<input type="text" value="██████@qnapp.com"/>	
Password:	<input type="password" value="●●●●"/>	Your password needs to be more than 5 characters and cannot be the same as your username. Do not choose a password that is a common word, or can otherwise be easily guessed.
Confirm Password:	<input type="password" value="●●●●"/>	

About You (optional)

Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!

How did you hear about us:	<input type="text" value="—"/>	We do not sell your account information to anyone, including your email address.
Details:	<input type="text"/>	

After you have created an account, a confirmation mail will be sent to your email address.

Account Created

Your account, `qnappqnap`, has been created. Directions for activating your account have been sent to your email address: `██████@qnapp.com`. To complete registration, please follow the directions you receive within 48 hours.

You should receive the confirmation email within a few minutes. Please make certain that your spam filtering allows messages from `support@dyndns.com` to be delivered. If you have not received this email within an hour or so, request a [password reset](#). Following the instructions in the password reset email will also confirm your new account.

Thanks for using DynDNS!

After confirming the registration, login the DDNS service.

Login

Account Login	Username: <input type="text" value="qnappqnap"/>	Password: <input type="password" value="●●●●●●"/>	<input type="button" value="Login"/>
---------------	--	---	--------------------------------------

The account summary is shown.

The screenshot shows the DynDNS account summary page for user 'qnapqnap'. The page has a yellow header with the DynDNS logo and navigation links: About, Services, Account, Support, and News. The user is logged in as 'qnapqnap' with links for 'My Services', 'My Cart', and 'Log Out'. A left sidebar contains navigation options: My Account, My Services, Account Settings, Billing, My Cart (0 items), and a search box. The main content area is titled 'Account Summary for qnapqnap' and is divided into three columns: 'My Services', 'Billing', and 'Account Settings'. Each column has a description and a list of links. The footer contains copyright information: © 1998-2008 Dynamic Network Services, Inc. - Legal Notices - Contacts.

DynDNS Logged In User: **qnapqnap**
[My Services](#) - [My Cart](#) - [Log Out](#)

About Services Account Support News

My Account
My Services
Account Settings
Billing
My Cart 0 items
Search

Account Summary for qnapqnap

My Services	Billing	Account Settings
View, modify, purchase, and delete your services.	Update your billing information, complete a purchase, and view invoices.	Update your email address, set preferences, and delete your account.
My Zones Add Zone Services My Hosts Add Host Services Spring Services Account Upgrades MailHop Outbound Network Monitoring SSL Certificates Recursive DNS Support Premier Support Contact Support DNS Service Level Agreement	View Shopping Cart Active Services Order History Billing Profile and Vouchers Renew Services Auto Renew Settings Sync Expirations	Change Email Address Change Password Change Username Contact Manager Mailing Lists Move Services Preferences Close Account

© 1998-2008 Dynamic Network Services, Inc. - [Legal Notices](#) - [Contacts](#)

Go to 'Services' > 'Dynamic DNS'.

The screenshot shows the DynDNS website interface. At the top, the DynDNS logo is on the left, and the user is logged in as 'qaggnap' with links for 'My Services', 'My Cart', and 'Log Out'. A navigation bar contains 'About', 'Services' (highlighted with a red box), 'Account', 'Support', and 'News'. A left sidebar lists services like 'DNS Services', 'Domain Registration', 'SSL Certificates', 'MailHop Services', 'Network Monitoring', 'Spring Server™', 'URL Forwarding', 'Pricing', and 'My Cart Items'. The main content area is titled 'Services' and contains a paragraph about superior domain name services and technical support. Below this is a 'DNS Services' section with four icons: 'Dynamic DNS' (highlighted with a red box), 'Custom DNS', 'Recursive DNS', and 'Secondary DNS', each with a brief description.

Click 'Get Started' to create a host.

The screenshot shows the 'Dynamic DNS' page. The title 'Dynamic DNS' is at the top. Below it, a paragraph explains that Dynamic DNS (DDNS) allows creating a hostname that points to a dynamic IP or static IP address, and that the service is free. Two buttons, 'Get Started' and 'Manage Hosts', are visible, with 'Get Started' highlighted by a red box. A 'Screenshot' section shows a small image of a DNS configuration interface. Below this is a 'Capabilities and Features' section with a bulleted list of features.

Dynamic DNS

Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. We also provide an update mechanism which makes the hostname work with your dynamic IP address. **We continue to offer this service free** to the Internet community as we have done so for nearly 10 years.

Get Started

Manage Hosts

Screenshot

Capabilities and Features

- Get five (5) hostnames in [88 available domains](#) for free.
- Create wildcard CNAME **,yourhost.dyn dns.org for yourhost.dyn dns.org*.
- Forward web requests or mark host offline for maintenance or downtime.
- Configure MX records for flexible mail routing.
- Update host using [ddns update clients](#) for a wide variety of platforms.
- Modify DNS TTL values for fast propagation or reliable static IP caching.
- Deliver your DNS records to 5 DNS servers in 5 tier-1 datacenters around the globe.
- Query volume up to 648,000 queries/month

Our **free industry-leading e-mail support** is ready to help you setup your dynamic or static DNS so you can host a website, remotely connect to your machine, and run a mail server. We also offer other premium features with our [Account Upgrade](#) service.

Enter the settings to create a new host.

Tip: The 'IP Address' refers to your current WAN IP. You may check the information from <http://www.ip-lookup.net/>. In most of the cases, it is useful for you to know your public IP address when you are behind a NAT router.

Add New Hostname

[Host Services](#)

Note: You currently don't have Account Upgrades in your account. You cannot use some of our Host Service features. Please consider buying Account upgrade that make this form full-functional and will add several other features. [Learn More...](#)

Hostname: .

Wildcard: Yes, alias **.hostname

Service Type: Host with IP address
 WebHop Redirect
 Offline Hostname

IP Address:
[Use auto detected IP address](#)
TTL value is 60 seconds

Mail Routing: Yes, let me configure

A new host is created.

Host Services

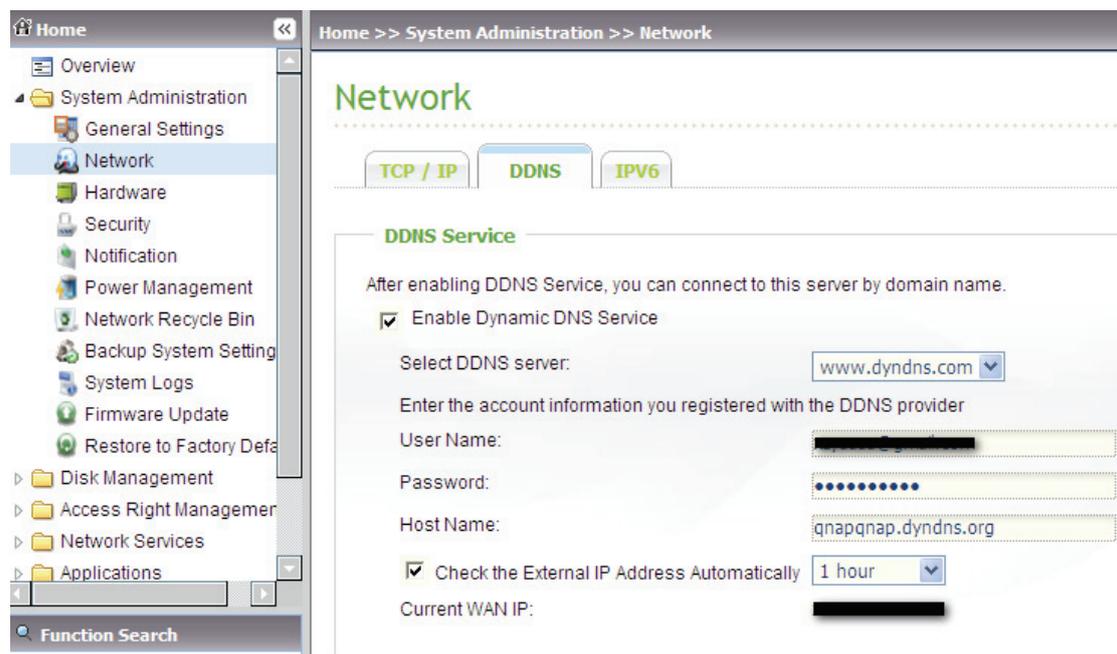
[Add New Hostname](#) - [Host Update Logs](#)

Hostname [qnapqnap.dyndns.org](#) created.

Hostname	Service	Details	Last Updated
qnapqnap.dyndns.org	Host	219.85.63.13	Sep. 05, 2008 3:53 AM

Login your QNAP NAS and go to 'System Administration' > 'Network' > 'DDNS'. Enter the DDNS settings. Schedule the NAS to update the DDNS record periodically.

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



After you have finished the settings, you can connect to the NAS using the host name (qnapqnap.dyndns.org).

Port Forwarding

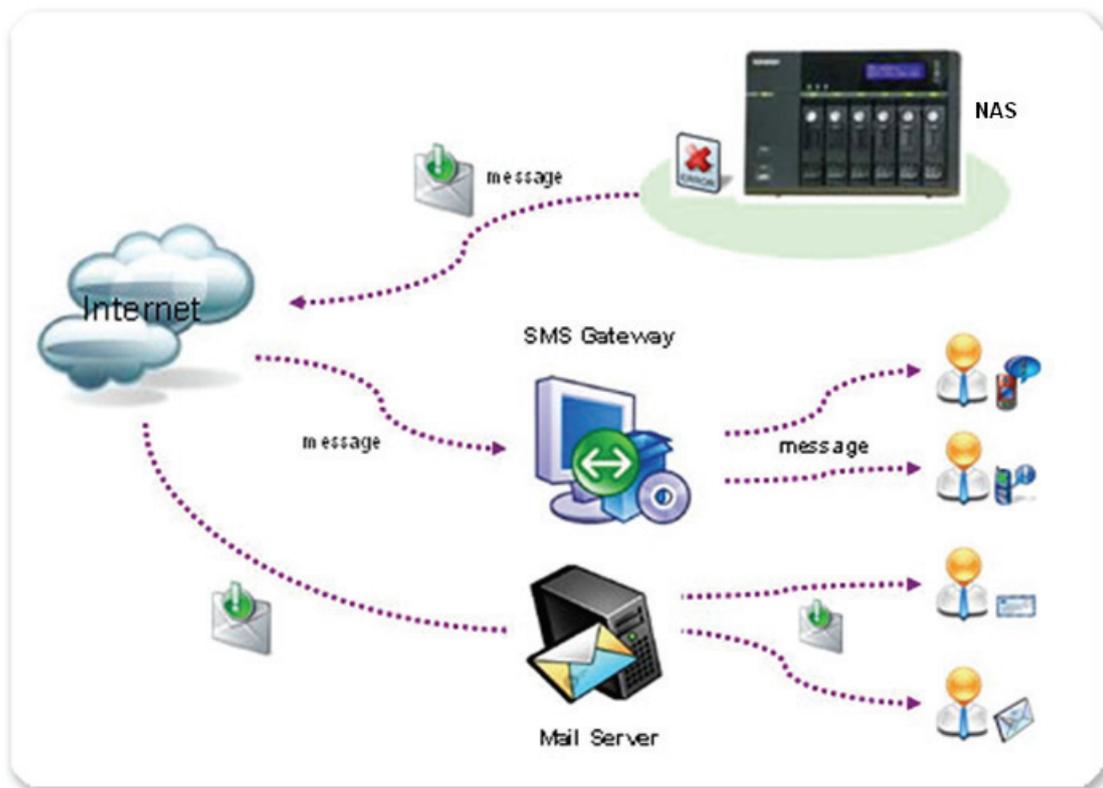
If your NAS is located behind an NAT router, you need to open the ports of some services on the NAT router and forward these ports to the fixed LAN IP of the NAS so that you can connect to the services correctly from the Internet. This function is available on most routers in the market and is often 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 (BitTorrent download)	6881–6999
Remote replication (Rsync)	873
Telnet	13131
SSH	22
SSL	443
SMTP	25
Samba	445
MySQL	3306
TwonkyMedia	9000

Appendix B. Set SMS and Email Alert

QNAP NAS supports SMS and email alert to inform the users of system error or warning. SMS is the abbreviation of Short Message Service which is known for the mobile text message service. By subscribing with the SMS service providers you are able to set up QNAP NAS to send SMS to the designated mobile phones in the event of system warning or errors. This demonstration shows you how to set up both the SMS and email alert on your NAS. See below for the usage diagram.

*Note: TS-109/ 209/ 409/ 409U series only support email alert.



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 ▼

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: 

INTERNATIONAL

Local Coverage Account: 

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:

Username:

ClientID:

Password:


[Lost password?](#)

Next you will need to 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

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:

While still logged in with Clickatell, go to 'Manage my Products' and select 'HTTP' from 'My Connections' dropdown menu.

Central Home My Settings Manage my Products Billing Message Reports Help

Manage my Products

- My Connections
 - Converters
 - Two-Way Messaging
- Application Forms
 - Two-Way Messaging
 - SA Shortcode MO
 - Namibia Shortcode
 - USA Shortcode
 - USA Shortcode MFS
 - UK Shortcode
 - Canada Shortcode
 - Clickatell ICM

Test Message in Message Box

Please Note that Clickatell pre-populates all test credits with a standard test message. Once you have purchased Clickatell credits, the test message will be removed and you will be able to send personalized text messages.

Buy SMS Credits

My Connections:

Add Connection

- Add Connection
- HTTP
- SMTP
- FTP
- XML
- COM
- SMPP
- SOAP

... a quick overview of each connection type. Also take a look at a comparison of [Clickatell](#) and [supported message types](#)

... popular connection, HTTP is one of the simpler forms of communicating to the Clickatell API. It is [HTTP/Internet Post](#). [Add connection](#)

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.

HTTP API

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.

Add HTTP API - Bold Items Required

Name:

IP Lock Down:

Dial Prefix:

Callback Type:

Callback Url:

Callback Username:

Callback Password:

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>
TS-639-Pro	HTTP	3176048	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.

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 the QNAP NAS web interface. The breadcrumb navigation at the top reads 'Home >> System Administration >> Notification'. The left sidebar menu has 'Notification' highlighted with a red box. The main content area is titled 'Notification' and contains three tabs: 'CONFIGURE SMTP SERVER', 'CONFIGURE SMSC SERVER', and 'ALERT NOTIFICATION'. The 'CONFIGURE SMSC SERVER' tab is active, showing the 'Configure SMSC Server' configuration form. The form includes a description: 'You can configure the SMSC settings to send instant system alerts via the SMS service provided by the SMS provider.' The configuration fields are: 'SMS Service Provider' (dropdown menu set to 'Clickatell' with a link to 'http://www.clickatell.com'), 'Enable SSL Connection' (checkbox checked), 'SSL Port' (text box with '443'), 'SMS Server Login Name' (text box with 'qnap'), 'SMS Server Login Password' (password field with 7 dots), and 'SMS Server API_ID' (text box with '3176048'). An 'APPLY' button is located at the bottom right of the form.

Next go to 'System Administration' > 'Notification' > 'Alert Notification' and enter your mobile number.

Home >> System Administration >> Notification

Welcome admin | Logout English

Notification

[CONFIGURE SMTP SERVER](#) [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:

Send system warning alert by:

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.

SMS Notification Settings

Country Code:

Cell Phone No. 1: +886

Cell Phone No. 2: +886

[SEND A TEST SMS MESSAGE](#)

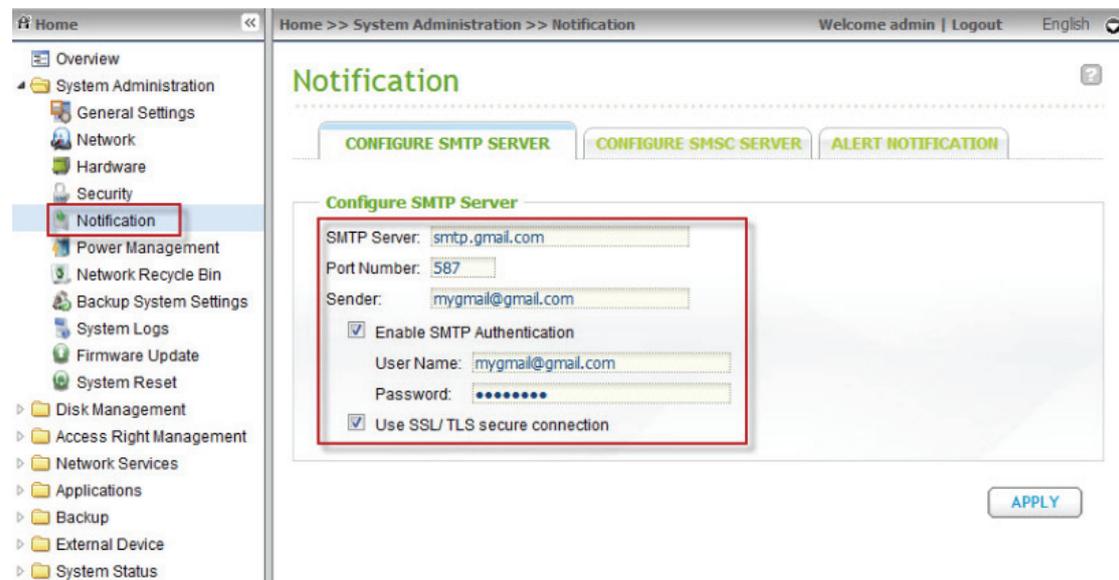
Note: You must configure the SMSC server to be able to send SMS notification properly.

[APPLY](#)

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 the SMTP server and email alert

Go to 'System Administration' > 'Notification' > 'Configure SMTP server' and enter a valid SMTP information. We will use Gmail as the SMTP service provider in this example.



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. You can test if the email sending process works by clicking 'SEND A TEST E-MAIL'.

Now no matter if you are out at work or away from home you will still be notified of any NAS error and warning right away by either an SMS sent to your mobile or an email and be able to act in case of any unexpected events.

Appendix C. Online RAID Capacity Expansion & Online RAID Level Migration

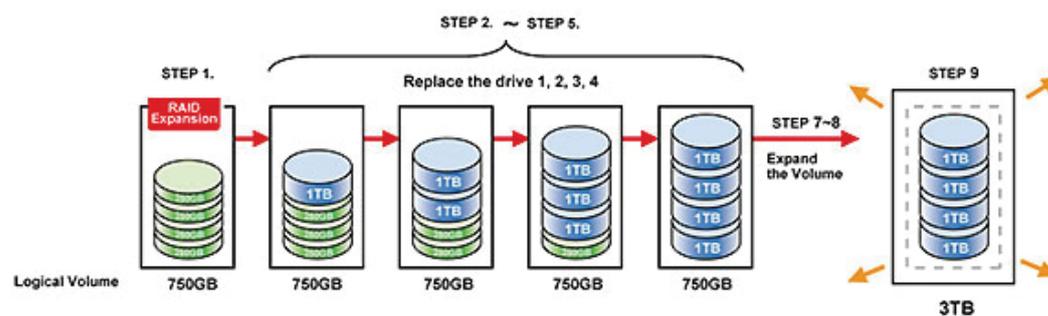
Online RAID Capacity Expansion

Scenario

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

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'.

The screenshot shows the RAID Management interface. On the left is a navigation menu with 'RAID Management' selected. The main content area is titled 'RAID Management' and contains a table of 'Current Disk Volume Configuration'. The table has columns for Volume, Total Size, Bitmap, Status, and Description. One row is highlighted: 'RAID 5 Disk Volume: Drive 1 2 3 4 5' with a total size of 931.56 GB and a status of 'Ready'. Below the table are several buttons: 'EXPAND CAPACITY', 'ADD HARD DRIVE', 'MIGRATE', 'CONFIGURE SPARE DRIVE', 'DISABLE BITMAP', and 'RECOVER'. The 'EXPAND CAPACITY' button is highlighted with a red box. A note above the table states: '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.'

Click 'Change' for the first HDD to be replaced. Follow the instructions to proceed.

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="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

Tip: After replacing the HDD, the description field shows the message 'You can replace this drive'. This means you can replace the HDD to a larger one or skip this step if the HDD 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 HDD 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 HDD, wait for the NAS to beep. The system starts 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 finishes, repeat the steps above to replace other HDD.

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 HDD and rebuilding completes, you can click 'EXPAND CAPACITY' to execute RAID expansion.

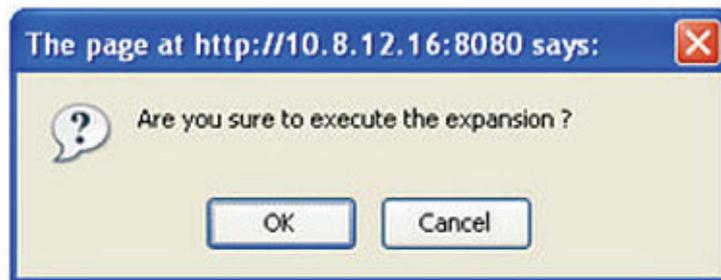
RAID Management ?

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

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**

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 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 expansion has finished, the new capacity is shown and the status is 'Ready'. You can start to use the larger capacity. (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
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.

Online RAID Level Migration

Scenario

During the initial setup of TS-509 Pro, you bought a 1TB HDD and configured it as single disk. 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 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.

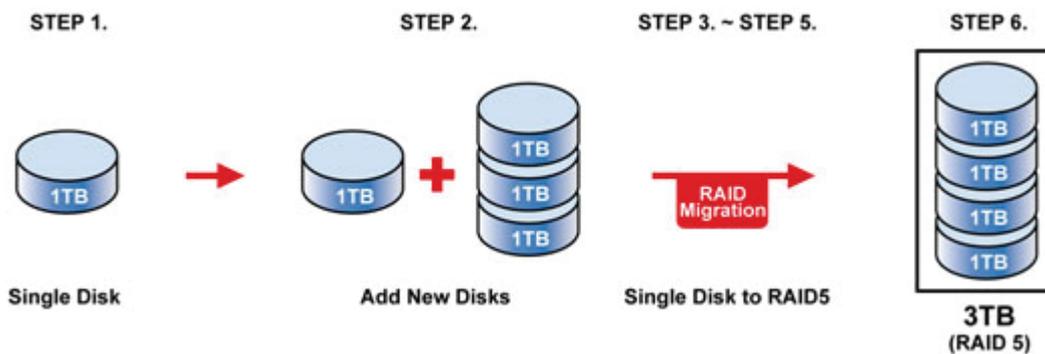
Using online RAID level migration, you can install one HDD for setting up TS-509 Pro and upgrade the RAID level in the future. The migration process can be done without turning off the server. All the data will be retained.

You can do the following with online RAID level migration:

Migrate the system from single disk to RAID 1, RAID 5, or RAID 6

Migrate the system from RAID 1 to RAID 5 or RAID 6

Migrate the system from RAID 5 with 3 HDD to RAID 6



You need to:

- Prepare the HDD 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 HDD).

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 GKA0	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	---

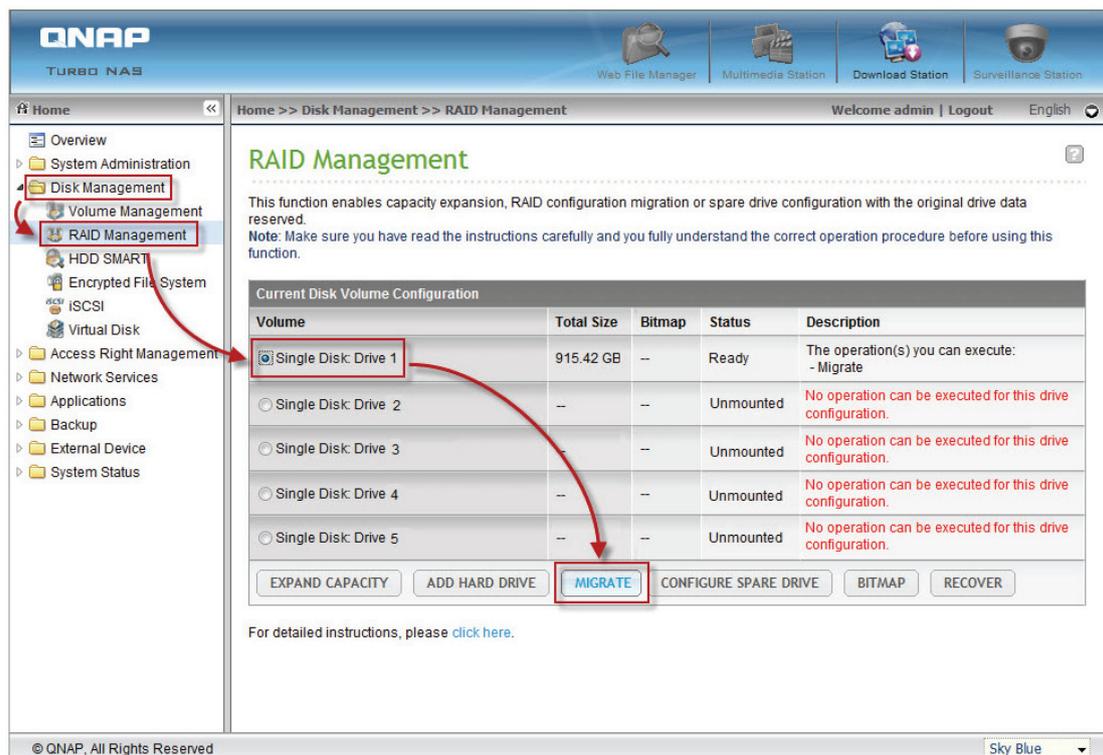
Current Disk Volume Configuration: Logical Volumes				
Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 1	EXT3	931.51 GB	524.68 GB	Ready
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				

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

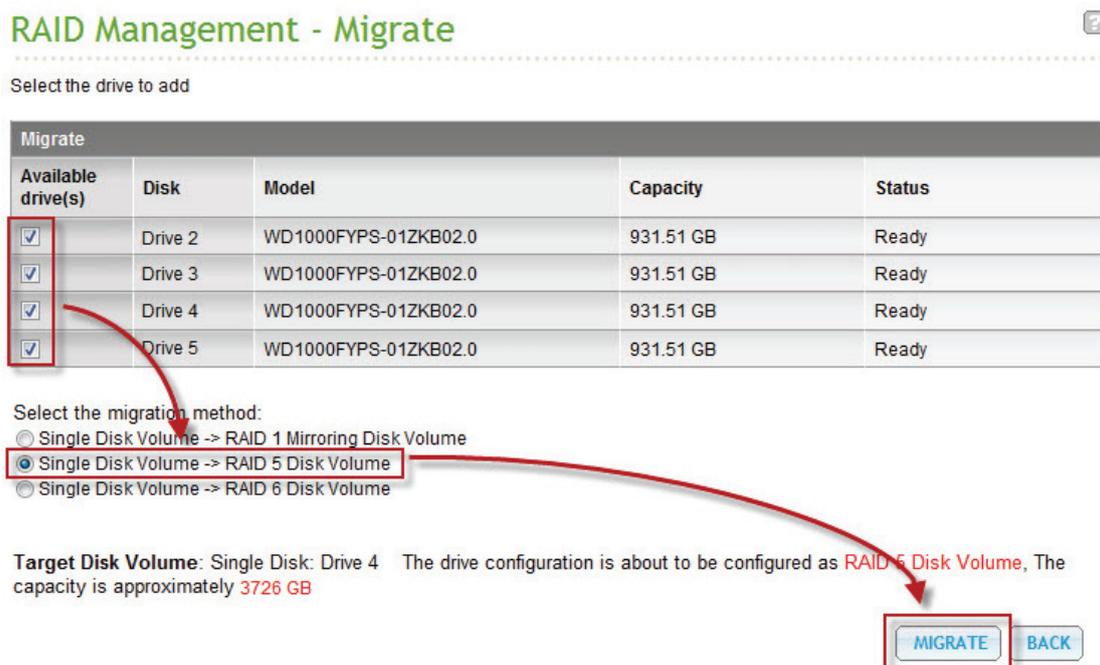
Current Disk Volume Configuration: Physical Disks					
Drive 1	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKA0	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKA0	931.51 GB	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
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				
Single Disk: Drive 2	EXT3	--	--	Unmounted
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				
Single Disk: Drive 3	EXT3	--	--	Unmounted
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				
Single Disk: Drive 4	EXT3	--	--	Unmounted
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				
Single Disk: Drive 5	EXT3	--	--	Unmounted
<div style="text-align: right;"> FORMAT NOW CHECK NOW REMOVE NOW </div>				

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



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



Note that all the data on the selected HDD will be cleared. Click 'OK' to confirm.



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

Current Disk Volume Configuration: Physical Disks					
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

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

Note: 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 is shown (RAID 5 now) 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](#).

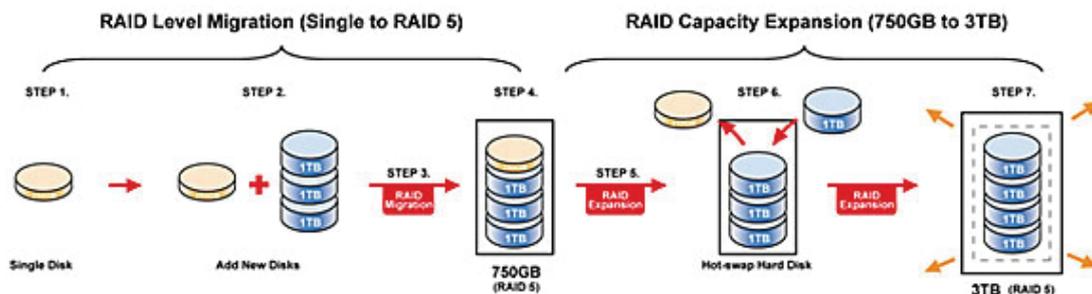
The process may take from hours to tens of hours to finish depending on the HDD size. You can connect to the web page of the NAS to check the status later.

Use Online RAID Capacity Expansion and RAID Level Migration together

Scenario

You had a tight schedule to set up the file server and FTP server. However, you had only one 250GB HDD. 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 TS-509 Pro. You now planned to upgrade the disk configuration of TS-509 Pro to RAID 5 and expand the total storage capacity to 3TB with all the original data retained after the HDD are purchased.

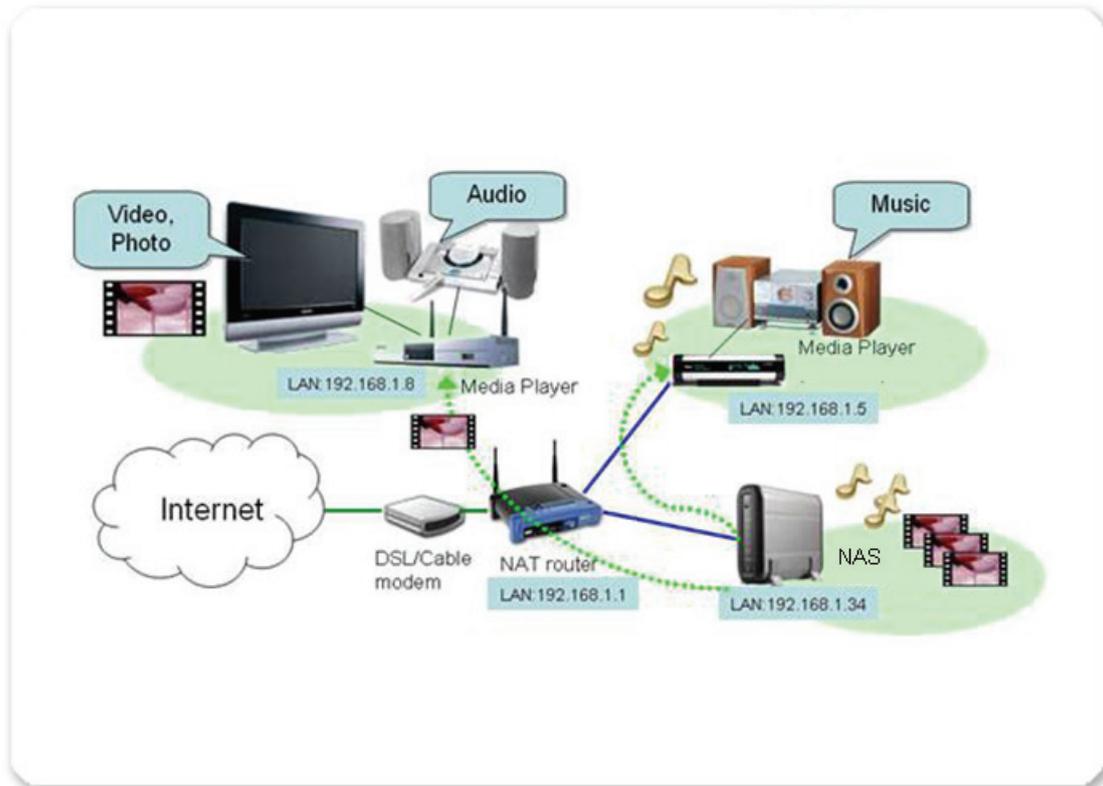


Execute online RAID level migration to migrate the system from single disk to RAID 5. The total storage capacity will be 750GB, RAID 5 (with one 250GB HDD and three 1TB HDD, the disk usage will be $250\text{GB} \times 4$ for RAID 5.). You can refer to the previous step for the operation procedure.

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

Appendix D. Set up UPnP Media Server for Media Playing

This section shows you how to set up the UPnP media server on QNAP NAS to share the multimedia files to the media player on the local network and play them in your home entertainment system.



Enable UPnP Media Server

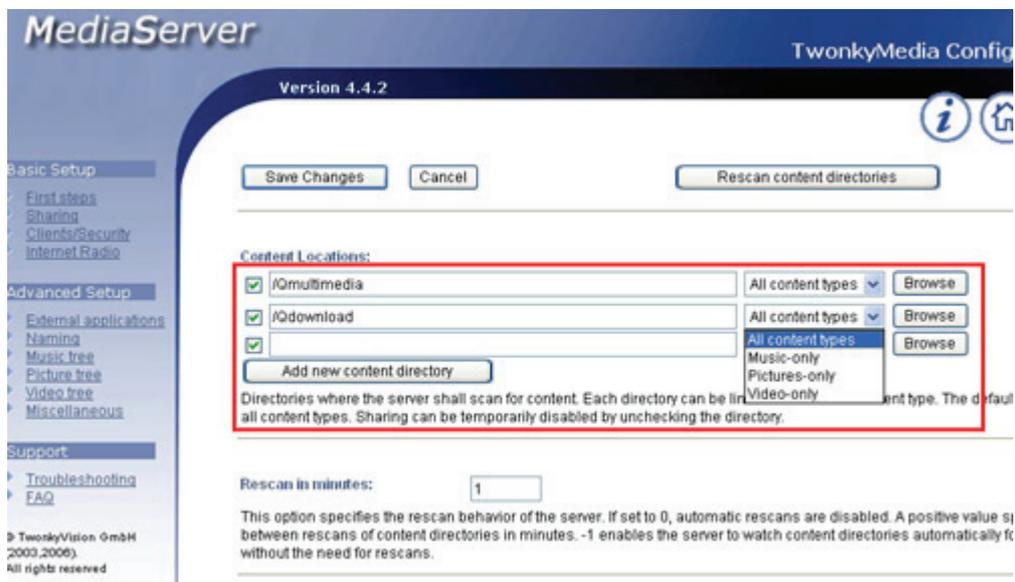
Go to 'Applications' > 'UPnP Media Server' and select the option 'Enabled UPnP Media Server' and click 'Apply'. The UPnP Media Server function is now ready.



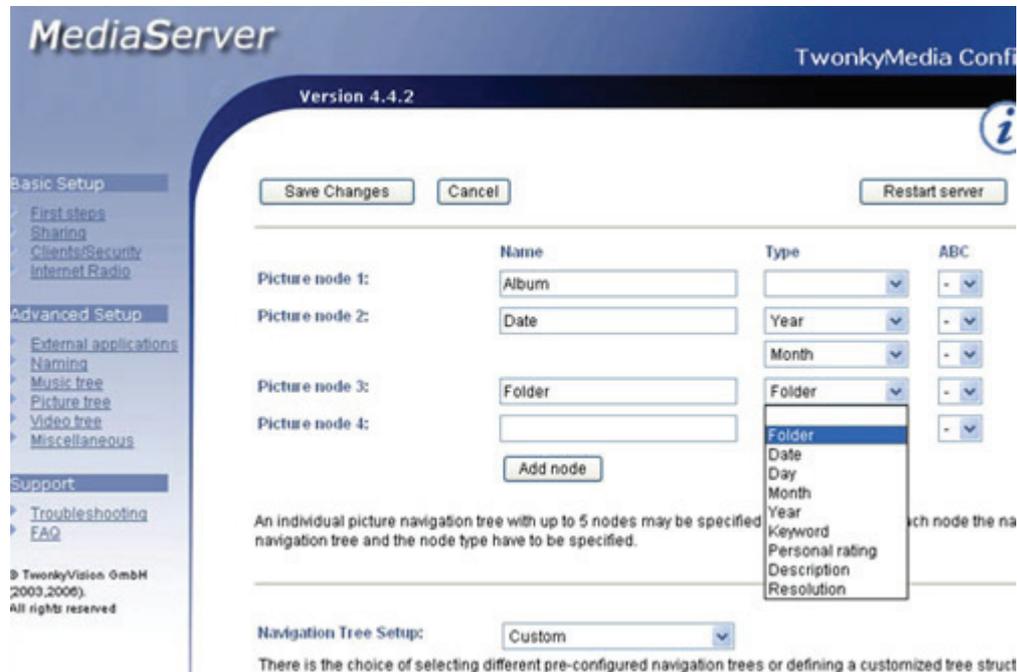
Set up the TwonkyMedia Server

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 your 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 the media player

About physical wiring

We use a high definition (HD) media player with QNAP NAS in 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.

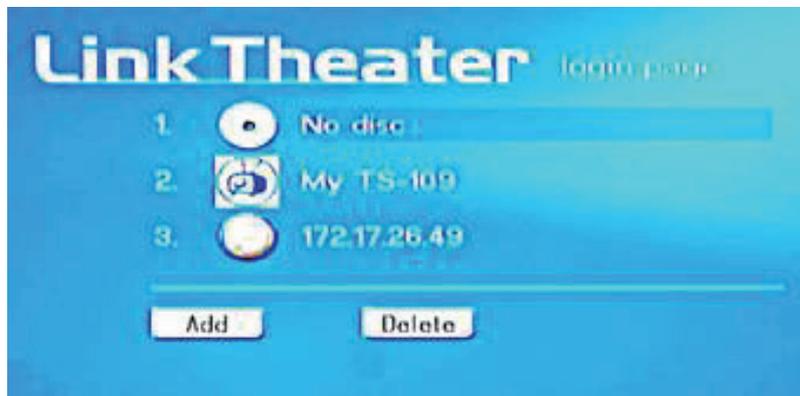


Example 1 (Buffalo LinkTheater)

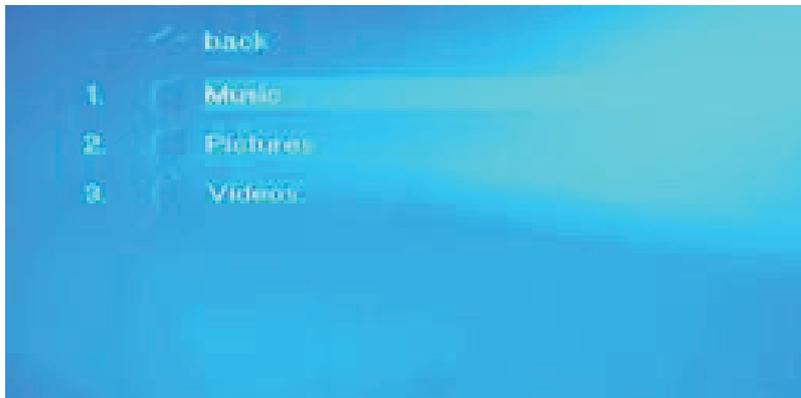
In this example, the video out and audio out cables are connected to the TV. You can also connect audio out to your stereo acoustic system.



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.



Appendix E. 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

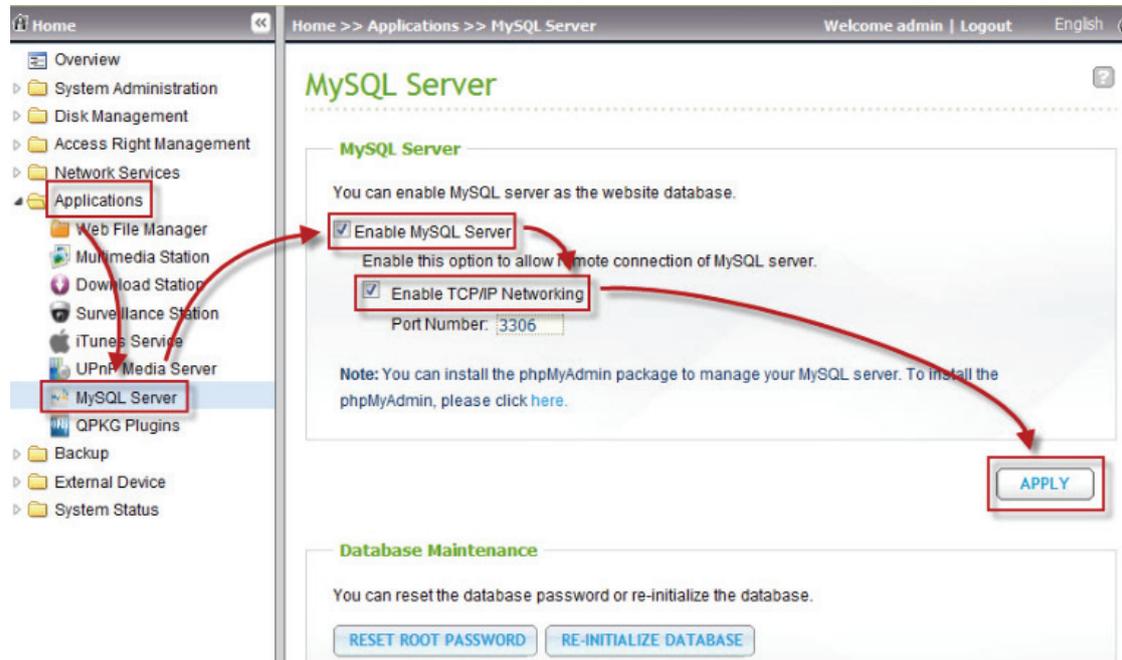
Login the administration page of the NAS and go to 'Network Services' > 'Web Server'. Select the option 'Enable Web server' and click 'Apply'.

The screenshot displays the QNAP NAS administration interface. The left sidebar shows a navigation menu with 'Network Services' expanded, and 'Web Server' selected. The main content area is titled 'Web Server' and contains the following configuration options:

- Enable Web Server
- Port Number: 80
- register_globals: On Off

Below these options, there is a link to the Web Server: <http://192.168.1.3:80/>. At the bottom right of the configuration area, there is an 'APPLY' button. Below the main configuration area, there is a section for 'php.ini Maintenance' with a checkbox for 'php.ini Maintenance'.

Next go to 'Applications' > 'MySQL Server' and select both 'Enable MySQL Server' and 'Enable TCP/IP Networking' then click 'Apply'.



Create a database for phpBB3 in phpMyAdmin

Prior to installing phpBB3, create a new database for it and we will use phpMyAdmin to create the database so install phpMyAdmin QPKG if you do not have it running on your NAS yet. Once installed point your browser to **http://NAS-IP/phpMyAdmin/** and enter the user name and password to login (default user name and password is **root/admin**). You can also select your preferred language.



Welcome to phpMyAdmin

Language
English

Log in

Username: root

Password: ●●●●

Go

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.

MySQL 127.0.0.1

Create new database

phpbb3 utf8_unicode_ci

Create

MySQL connection collation: utf8_unicode_ci

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 your Qweb or Web share folder.

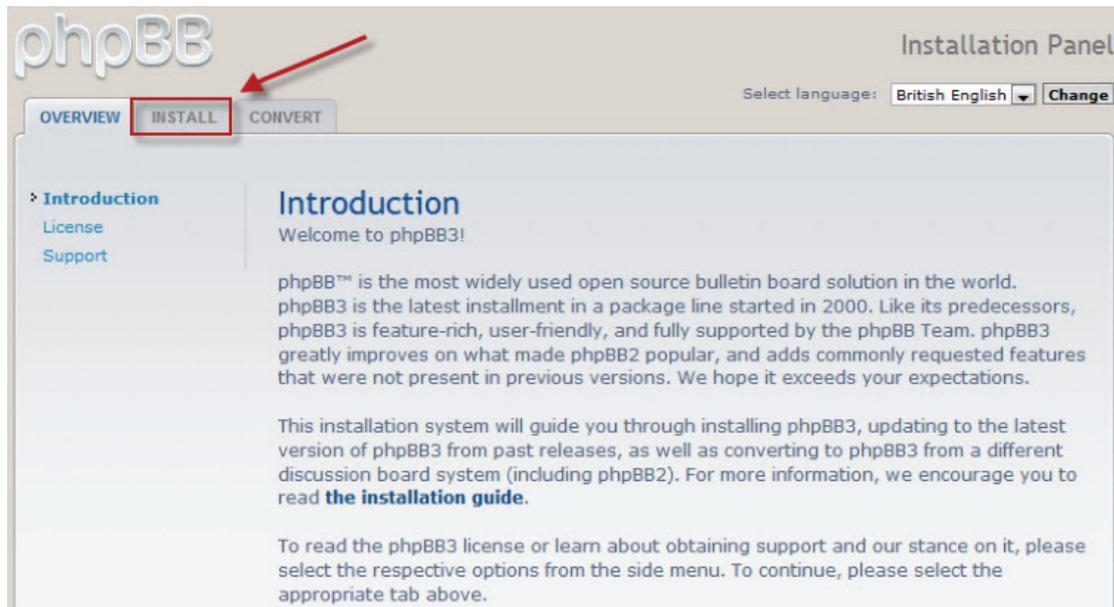
[Full Package]

Contains entire phpBB3 source and english language files.
Best suited for new installations.

 [Download phpBB 3.0.5 \(zip\)](#)
Size: 2.22 MiB
md5sum: 69c4ec3f1495e518c6b8a5dac8549ab4

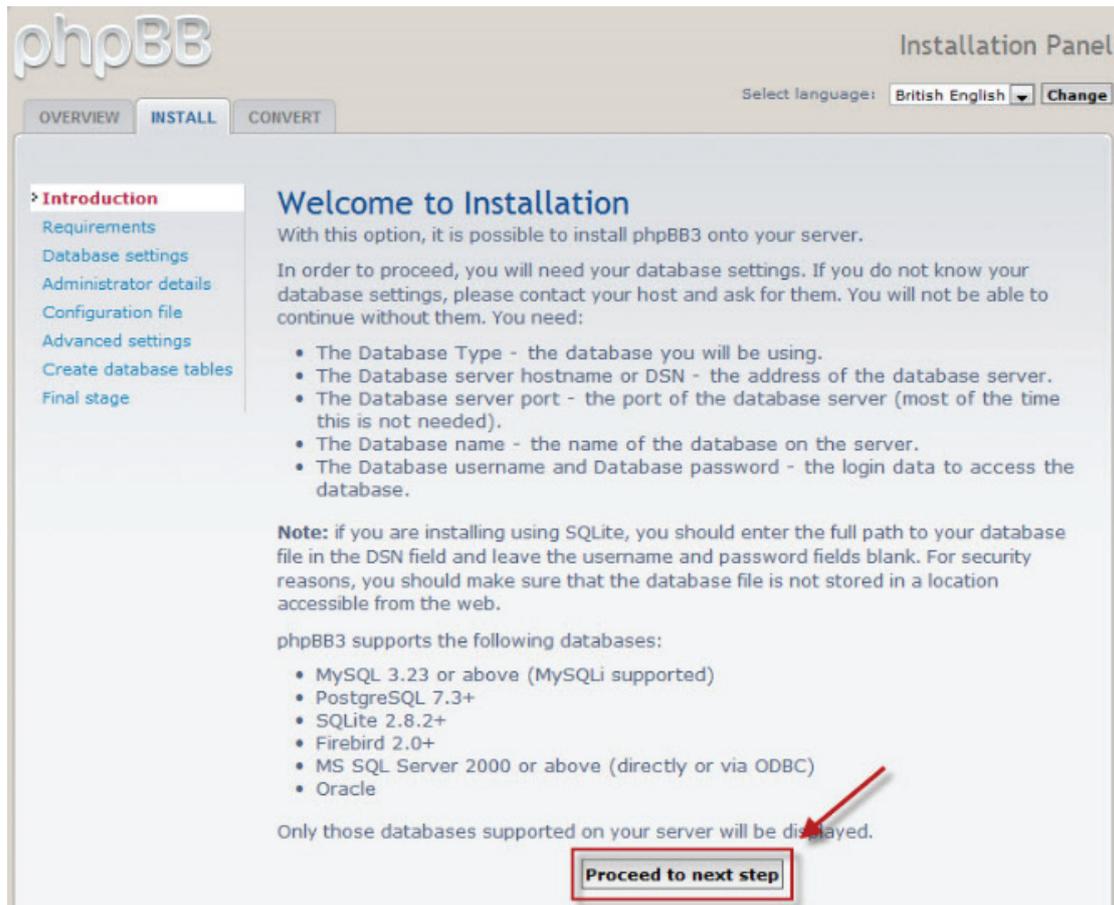
 [Download phpBB 3.0.5 \(bz2\)](#)
Size: 1.43 MiB
md5sum: 734b8f9c2390d5ccc8c971cfeb29da185

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 sidebar with 'Introduction', 'License', and 'Support'. 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'.



The screenshot shows the phpBB Installation Panel. At the top left is the phpBB logo, and at the top right is the text 'Installation Panel'. Below the logo are three tabs: 'OVERVIEW', 'INSTALL', and 'CONVERT'. To the right of these tabs is a language selection dropdown set to 'British English' with a 'Change' button. The main content area is titled 'Welcome to Installation' and contains the following text:

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.

A red arrow points to the 'Proceed to next step' button, which is highlighted with a red box.

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 hostname, 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 (blank), 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.

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'.

The screenshot shows the phpBB Installation Panel with the 'INSTALL' tab selected. The 'Database connection' section is active, and a green box highlights the 'Successful connection' message. A 'Proceed to next step' button is highlighted with a red box and an arrow pointing to it.

Specify the phpBB3 administrator username and password as well as a valid email address. Once done, click 'Proceed to next step'.

The screenshot shows the phpBB3 Installation Panel with the 'INSTALL' tab selected. The 'Administrator configuration' section is active, containing the following fields and instructions:

- Default board language:** A dropdown menu set to 'British English'.
- Administrator username:** A text input field containing 'admin'. Below it, the instruction reads: 'Please enter a username between 3 and 20 characters in length.'
- Administrator password:** A password input field with masked characters. Below it, the instruction reads: 'Please enter a password between 6 and 30 characters in length.'
- Confirm administrator password:** A second password input field with masked characters.
- Contact e-mail address:** A text input field containing 'admin@myforum.com'.
- Confirm contact e-mail:** A second text input field containing 'admin@myforum.com'.

A red box highlights the entire configuration area, and a red arrow points to the 'Proceed to next step' button located at the bottom center of the panel.

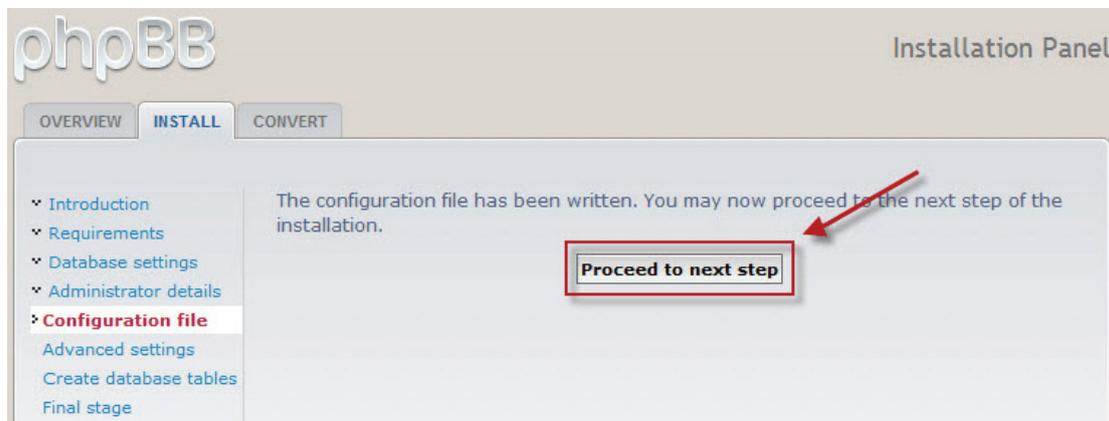
You should see 'Tests passed' and click 'Proceed to next step'.

The screenshot shows the phpBB3 Installation Panel with the 'INSTALL' tab selected. The 'Administrator details' section is active, displaying the following information:

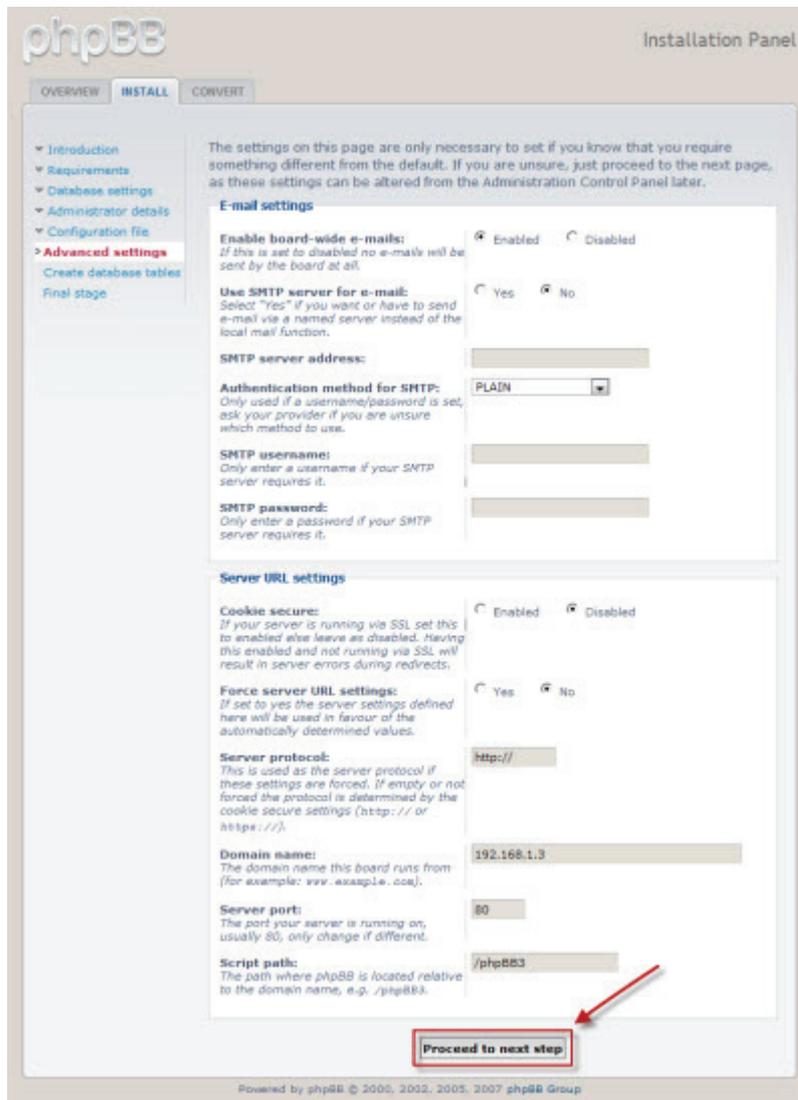
- Administrator details**
- Check administrator settings:** A green box with the text 'Tests passed'.

A red box highlights the 'Proceed to next step' button at the bottom center, with a red arrow pointing to it from the right.

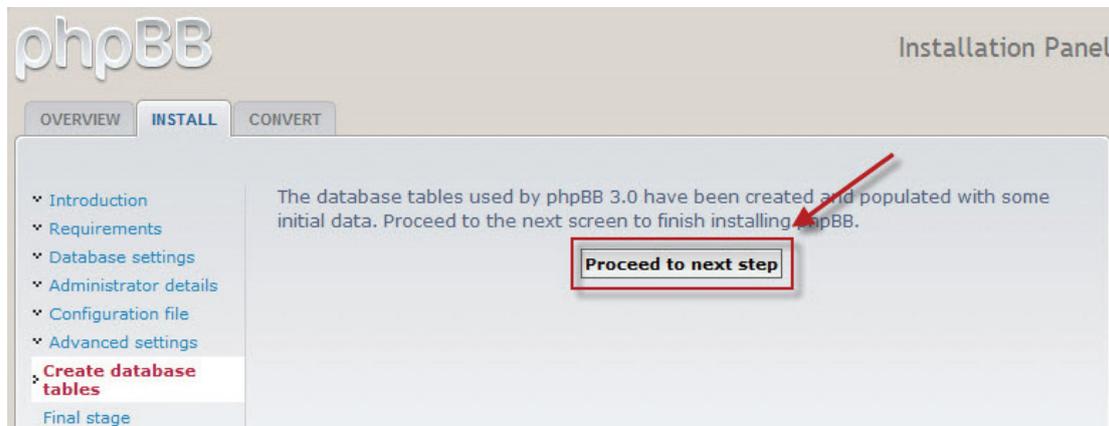
phpBB3 writes all the settings information to a configuration file (config.php) at this stage. Click 'Proceed to next step'.



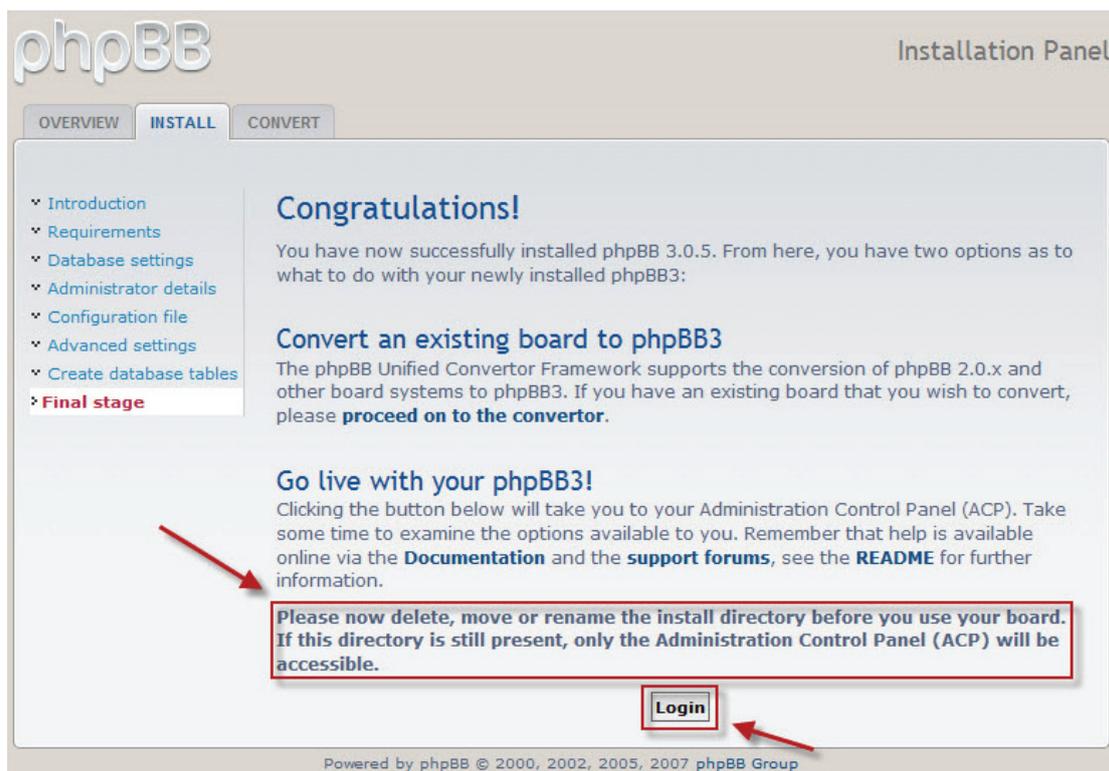
Specify advanced settings if you wish then click 'Proceed to next step'.



phpBB3 creates all the database tables and populates some initial data at this stage. Click 'Proceed to next step'.



Now there is one more thing you need to do is that you have to delete the installation folder located under the phpBB3 folder. Once deleted you can click 'Login' to enter the administration page of phpBB3.



This is the phpBB3 Administration Control Panel where you can perform all administrative tasks.

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
Purges all cache related items, this includes any cached template files or queries.

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	TYPE	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](#) ∨ 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](#)

Technical Support

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

Online Support: <http://www.qnap.com/>

MSN: q.support@hotmail.com

Skype: qnapskype

Forum: <http://forum.qnap.com/>

Technical Support in the USA and Canada:

Email: q_supportus@qnap.com

TEL: 909-595-2819 ext. 185

Address: 166 University Parkway, Pomona CA 9176

Service Hours: 08:00-17:00 (GMT- 08:00 Pacific Time, Monday to Friday)

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