QNAP Turbo NAS
Software User Manual

(Version: 4.3.x)

This manual is applicable to the following Turbo NAS models:

1-Bay	TS-131, TS-131P
2-Bay	TS-231, TS-231+, TS-231P, HS-251, HS-251+, TS-251, TS-251+, TS-251A, TS-251C, TS-253 Pro, TS-253A, TS-269L, TS-269 Pro
4-Bay	IS-400 Pro, TS-431, TS-431U, TS-431+, TS-431P, TS-431X, TS-431XU, TS-431XU-RP, TS-451, TS-451+, TS-451S, TS-451U, TS-451A, TBS-453A, IS-453S, TS-453S Pro (SS-453 Pro), TS-453 Pro, TS-453A, TS-453U, TS-453U-RP, TS-453mini, TS-453Bmini, TVS-463, TS-463U, TS-463U-RP, TS-469 Pro, TS-469L, TS-469U-RP, TS-469U-SP, TS-470, TVS-470, TS-470U-RP, TS-470U-SP, TS-470 Pro, TVS-471, TVS-471U, TVS-471U-RP, TVS-473
5-Bay	TS-531P, TS-531X, TS-563, TS-569 Pro, TS-569L
6-Bay	TS-651, TS-653 Pro, TS-653A, TVS-663, TS-669 Pro, TS-669L, TS-670 Pro, TS-670, TVS-670, TVS-671, TVS-673, TVS-682, TVS-682T2
8-Bay	TS-831X, TS-831XU, TS-831XU-RP, TS-851, TS-853 Pro, TS-853S Pro (SS-853 Pro), TS-853U, TS-853U-RP, TS-853A, TS-863U, TVS-863, TVS-863+, TS-863U-RP, TS-869 Pro, TS-869L, TS-869U-RP, TS-870 Pro, TS-870, TVS-870, TS-870U-RP, TVS-871T, TVS-871, TVS-871U-RP, TVS-873, TS-879 Pro, TS-879U-RP, TS-EC879U-RP, TS-EC880U(TS-EC880U-RP), TVS-EC880, TS-EC880 Pro, TS-EC880U R2, TVS-882, TVS-882T2, TVS-882ST2, TVS-882ST3
10-Bay	TS-1079 Pro, TVS-EC1080+, TVS-EC1080, TS-EC1080 Pro
12-Bay	TS-1231XU, TS-1231XU-RP, TS-1253U, TS-1253U-RP, TS-1263U, TS-1263U-RP, TS-1269U-RP, TS-1270U-RP, TVS-1271U-RP, TS-1279U-RP, TS-EC1279U-RP, TS-EC1279U-SAS-RP, SS-EC1279U-SAS-RP, TS-EC1280U(TS-EC1280U-RP), TVS-EC1280U-SAS-RP, TS-EC1280U R2, TVS-EC1280U-SAS-RP R2, TVS-1282, TVS-1282T2, TVS-1282T3

15-Bay	TVS-EC1580MU-SAS-RP, TVS-EC1580MU-SAS-RP R2
16-Bay	TS-1635, TS-1679U-RP, TS-EC1679U-RP, TS-EC1679U-SAS-RP, TS-EC1680U(TS-EC1680U-RP), TS-EC1680U R2, TVS-EC1680U-SAS-RP, TVS-EC1680U-SAS-RP R2, TS-1685, TDS-16489U
18-Bay	SS-EC1879U-SAS-RP, TES-1885U
24-Bay	SS-EC2479U-SAS-RP, TS-EC2480U(TS-EC2480U-RP), TS-EC2480U R2, TVS-EC2480U-SAS-RP, TVS-EC2480U-SAS-RP R2
30-Bay	TES-3085U

*Unless otherwise specified, the content of this manual applies to all the above NAS models.

*For user manuals of other Turbo NAS models and firmware versions, please visit http://docs.qnap.com

Table of Contents

Notice

- [Legal Notice and Disclaimer](#)
- [Regulatory Notice](#)
- [Document Annotation](#)
- [Safety Information and Precautions](#)

Legal Notice and Disclaimer

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 NAS. The product you purchased may not support certain functions dedicated to specific models.

Legal Notices

All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.
QNAP and the QNAP logo are trademarks of QNAP Systems, Inc. All other brands and product names referred to are trademarks of their respective holders.
Further, the ® or ™ symbols are not used in the text.

Disclaimer

Information in this document is provided in connection with QNAP products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in QNAP's terms and conditions of sale for such products, QNAP Assumes no liability whatsoever, and QNAP disclaims any express or implied warranty, relating to sale and/or use of QNAP products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

QNAP products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

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

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

Should you return any components of the NAS package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

Regulatory Notice

FCC Notice

QNAP NAS comply with different FCC compliance classes. Please refer the Appendix for details. Once the class of the device is determined, refer to the following corresponding statement.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Modifications: Any modifications made to this device that are not approved by QNAP Systems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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

- 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.

Modifications: Any modifications made to this device that are not approved by QNAP Systems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

CE Notice

QNAP Turbo NAS models comply with different CE compliance classes. Please refer to the table for details.

FCC	CE	NAS Models
Class A	Class A	TS-EC1679U-RP, TS-EC1279U-RP, TS-EC879U-RP, TS-1679U-RP, TS-1279U-RP, TS-1270U-RP, TS-1263U-RP, TS-1263U,TS-1253U-RP, TS-1253U, TS-879U-RP, TS-870U-RP, TS-863U-RP, TS-853U-RP, TS-453U-RP, TS-1079 Pro, TS-879 Pro, TS-863U, TS-853U, TS-463U, TS-463U-RP, TS-453U-RP, TS-453U, TS-451U, TS-431U, TVS-871U-RP, TVS-1271U-RP
Class B	Class B	TS-853S Pro, TS-453S Pro, TS-870 Pro, TS-853 Pro, TS-670 Pro, TS-653 Pro, TS-470 Pro, TS-453 Pro, TS-253 Pro, TS-431+, TS-231+, TS-451S, TS-870, TS-851, TS-670, TS-651, TS-470, TVS-863+, TVS-863, TVS-663, TVS-463, TVS-471, TVS-671, TVS-871,TS-451, TS-451+, TS-431, TS-251, TS-251+, TS-251C, TS-231, TS-131, TS-269H, TS-212P, TS-112P, HS-251, HS-251+, HS-210, TS-453mini, TS-563, IS-453S, TS-531P, TS-253A, TS-453A, TS-653A, TS-853A, TS-128, TS-228, TAS-168, TAS-268, TS-831X, TVS-682T, TVS-882T, TVS-1282T, TVS-682, TVS-882, TVS-1282

Document Annotation

Annotations in this document

- *Warning:* This indicates the instructions must be strictly followed. Failure to do so could result in injury to human body or death.
- *Caution:* This 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 indicates the information provided is important or related to legal regulations.

Safety Information and Precautions

1. The NAS can operate normally in the temperature of 0ºC–40ºC and relative humidity of 0%–95%. Ensure 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. Ensure the usage environment's temperature and humidity is suited for using electronics.
4. Unplug the power cord and all connected cables before cleaning. Wipe the NAS with a dry towel. Do not use chemicals or aerosols to clean the NAS.
5. Do not place any objects on the NAS during normal system operations and to avoid overheating.
6. Use the flat head screws in the product package to lock the hard disk drives in the NAS when installing the hard drives for proper operation.
7. Do not place the NAS near any liquid.
8. Do not place the NAS on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using the NAS. If unsure, contact your distributor or the local power company.
10. Do not place any object on the power cord.
11. Never attempt to repair the NAS. Improper disassembly of the product may expose you to electric shock or other risks. For repair-related enquiries, please contact your distributor.
12. Rackmount NAS models should only be installed in server rooms and maintained by authorized server managers or IT administrators. The server room should be sufficiently locked and only certified staff allowed to enter.

Warning:
- There is the danger of explosion if a 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.
- To avoid serious injuries **do NOT touch the fan inside the system.**

Getting Started

New NAS users are advised to follow the below steps to complete their NAS installation. For users who already own a QNAP NAS and would like to move the data to a new QNAP NAS, refer to Migrating NAS for detailed instructions.

For New NAS Users:
1. Hardware Installation
2. Software Installation
3. Getting Utilities
4. Connecting to the Shared Folders
5. Connecting to the NAS by Web Browser

For Existing NAS Users:
- Migrating NAS

Hardware Installation

After unpacking the NAS, first follow these instructions to install your hardware:

1. Install the hard drives. Before doing so, ensure the hard drives (HDDs) that you use are compatible with the NAS. Go to the Hard Disk Drive Compatibility List section for more details.

2. Connect the QNAP NAS to the same network as your PC and power it on. During your installation process, pay attention to LEDs and alarm buzzers to make sure that the NAS functions properly. Go to the Checking System Status section for more details.

Note: The steps above are also illustrated in the Quick Installation Guide (QIG) that can be found in the product package or QNAP website (http://start.qnap.com).

Hard Disk Drive Compatibility List

This product works with 2.5-inch and 3.5-inch SATA hard disk drives and/or solid-state drives (SSD) from major hard drive brands. For a full list of compatible drives, check the compatibility list on the QNAP website (http://www.qnap.com/compatibility).

Note: If you encounter a "Device not found" message, ensure that:
1. Your NAS has been powered on;
2. The network cable is connected to the NAS and the orange and green indicator lights on its LAN port(s) are blinking; and
3. The cloud key is correct.

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

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

Checking System Status

LED Display & System Status Overview

LED	Color	LED Status	Description
System Status	Red/ Green	Flashes green and red alternately every 0.5 sec	1) The hard disk drive on the NAS is being formatted. 2) The NAS is being initialized. 3) The system firmware is being updated. 4) RAID rebuilding is in process. 5) Online RAID capacity expansion is in process. 6) Online RAID level migration is in process.
		Red	1) The hard disk drive is invalid. 2) The disk volume has reached its full capacity. 3) The disk volume is going to be full. 4) The system fan is out of function (TS-119 does not support smart fan.) 5) An error occurs when accessing (read/write) the disk data. 6) A bad sector is detected on the hard disk drive. 7) The NAS is in degraded read-only mode (2 member hard drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read.) 8) Hardware self-test error.
		Flashes red every 0.5 sec	The NAS is in degraded mode (one member hard drive fails in RAID 1, RAID 5 or RAID 6 configuration.)
		Flashes green every 0.5 sec	1) The NAS is starting up. 2) The NAS is not configured. 3) The hard disk drive is not formatted.
		Flashes green every 2 sec	The NAS is in S3 Sleep Mode[1].
		Green	The NAS is ready.
		Off	All the hard disk drives on the NAS are in standby

LED	Color	LED Status	Description
			mode.
Power[1]	Green	Flashes green	The NAS is booting up.
		Green	The NAS is on and ready.
LAN	Orange	Orange	The disk data is being accessed from the network.
		Flashes orange	The NAS is connected to the network.
10 GbE	Green	Green	The 10GbE network expansion card is installed.
		Off	No 10GbE network expansion card is installed.
HDD	Red/ Green	Red	A hard drive read/write error occurs.
		Flashes green	The disk data is being accessed.
		Green	The hard drive can be accessed.
USB	Blue	Flashes blue every 0.5 sec	1) A USB device (connected to front USB port) is being detected. 2) A USB device (connected to front USB port) is being removed from the NAS. 3) The USB device (connected to the front USB port) is being accessed. 4) The data is being copied to or from the external USB or eSATA device.
		Blue	A front USB device is detected (after the device is mounted.)
		Off	1) No USB device is detected. 2) The NAS has finished copying the data to or from the USB device connected to the front USB port of the NAS.
eSATA	Orange	Flashes	The eSATA device is being accessed.
		Off	No eSATA device can be detected.

[1]This feature is only supported by certain NAS models. Visit http://www.qnap.com for more details.

Alarm Buzzer

The alarm buzzer can be disabled in "Control Panel" > "System Settings" > "Hardware" > "Buzzer".

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

Software Installation

After installing the NAS hardware, proceed to software installation. There are three approaches for software installation:

1. Smart Installation Guide
2. Cloud Installation
3. HDMI Installation

Online installation and cloud installation are available for all new NAS models. All users are encouraged to use cloud and online installation if possible. Contact our technical support department if any problem arises during the installation process (http://www.qnap.com/support.)

Smart Installation Guide

Follow the steps in this section to complete online installation for your NAS:

1. Go to http://start.qnap.com.
2. Choose the number of HDD bays and the model of your NAS and click "Start Now".
3. Click "Hardware" and follow the on-screen instructions to get hardware ready.
4. Scroll down to "Install firmware" and click "Local Installation".
5. Choose your operating system to download, install and run Qfinder Pro.
6. After installing Qfinder Pro, launch it to search for your NAS. Double click on your NAS in Qfinder Pro to start the Smart Installation Guide. Follow the on-screen instructions to the built-in Qfinder Pro Setup Wizard will guide you along the way to complete the firmware installation.
7. Proceed to log into QTS with your account username and password to log in (QTS is the operating system for the Turbo NAS.)

Cloud Installation

Follow the steps in this section to complete cloud installation for your NAS:

1. Connect your NAS to the Internet, and on your PC, go to "install.qnap.com".
2. Enter the cloud key (cloud key can be found from the sticker on top of your QNAP NAS) and click "Enter".
3. Login to or register for myQNAPclould account. An activation email will be sent for new accounts. Click Confirm Registration in email to activate account.
4. Enter a name for your QNAP NAS. This name will be used to remotely access your device. Click Next.
5. Install hard drives on your Turbo NAS if you have not already done so.
6. On the Welcome page, click Start Smart Installation Guide to start the NAS installation process.
7. On the Name / Password page, enter your NAS name and admin password. Click Next.
8. On the Date / Time page, select your preferred time and date settings. Click Next.
9. On the Network page, enter your network settings. Click Next.
10. On the Services page, select which OS features you would like enabled. Multiple selections are allowed. Click Next.
11. On the Multimedia page, select if you would like to enable multimedia functions immediately after set up. Multiple selections are allowed. Click Next.
12. On the Disk page, select if you would like to configure disks now or later. Click Next.
13. On the Summary page, review your settings. Click Next if settings are correct. Click Back to make changes.

Note: If you encounter a "Device not found" message, ensure that:
1. Your NAS has been powered on;
2. the network cable is connected to the NAS and the orange and green indicator lights on its LAN port(s) are blinking; and
3. The cloud key is correct.

HDMI Installation

Follow the steps in this section to complete the HDMI installation for your NAS:

1. Connect the NAS to an HDMI display.

2. Follow the onscreen instructions to complete the firmware installation.

3. Choose to install HD Station or log into QTS with QTS account username and password (QTS is the operating system for the NAS.)

> **Note:**
> - This installation is restricted to NAS models with an HDMI port.
> - The default login ID and password of the NAS are both "admin".

Getting Utilities

Visit http://www.qnap.com/ and go to "Support" > "Download" > "Utilities" and choose to download and install the utilities on your PC.

Connecting to NAS Shared Folders

After installing the hardware and software, it is time to connect to the shared folders on the NAS. Refer to these links for the connection setup:

- Connecting to NAS shared folders in Windows
- Connecting to NAS shared folders in Mac or Linux

Windows

There are two methods for connecting to shared folders of the NAS when using Windows:

Method 1: Connect to the shared folders of the NAS by using QNAP Qfinder Pro
1. Launch QNAP Qfinder Pro. Select your NAS and then click "Tool" > "Map Network Drive".
2. Select a shared folder on the NAS to be mapped as a network drive and click "Map Network Drive".
3. Enter the username and password to connect to the NAS and click "OK".
4. Select a drive in the OS to map the folder chosen in Step 2 and click "Finish".
5. The mapped folder will appear when opening the File Explorer in Windows.

Note: Alternatively, you can use the Storage Plug & Connect Wizard to connect to NAS shared folders. The steps:
1. Launch QNAP Qfinder Pro;
2. Select "Storage Plug & Connect" under "Connect";
3. Check "Login with username and password" and enter the username and password;
4. Click a NAS shared folder;
5. Click "Map the Network Drive".

Method 2: Connect to the shared folders of the NAS by using File Explorer or Run
1. Open the Windows File Explorer, click on "Network" on the left and find the workgroup of the NAS. If the NAS cannot be found, browse the whole network to search for the NAS. Double click the name of the NAS to connect to it, or use the Run function in Windows (Windows key + R). Enter \\NAS_name or \\NAS_IP.
2. Enter the default administrator name and password (the default login ID and password are both "admin".).
3. Upload files to the shared folders.

Mac or Linux

Mac Users

There are two methods to connect shared folders on a NAS:

Method 1: Using QNAP Qfinder Pro

1. Launch QNAP Qfinder Pro, select your NAS, and go to "Connect" > "Open in File Explorer".
2. Enter your login ID and password.
3. Select the folder you want to mount and click "OK".
4. The folder is mounted.

Method 2: Connecting to Server

1. Choose "Go" > "Connect to Server".
2. Enter the NAS IP address.
3. Enter your login ID and password.
4. Select the folder you want to mount and click "OK".
5. The folder is mounted.

Linux Users

On Linux, run the following command:

> **mount -t nfs <NAS IP>:/<Shared Folder Name> <Directory to Mount>**

For example, if the IP address of the NAS is 192.168.0.1, to connect to the shared folder "public" under the /mnt/pub directory, use the following command:

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

Log into the NAS with the specified user ID, use the mounted directory to connect to the shared folders.

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

Connecting to NAS by Web Browser

To connect to the NAS by a web browser, follow these steps:

1. Enter http://NAS IP:8080 in the web browser. Or if using QNAP Qfinder Pro, simply double click on the NAS to open the login page.

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

2. Enter the administrator's login id and password. Enable "Secure login" (Secure Sockets Layer login) to allow a secure connection to the NAS. If a user without administration rights logs into the NAS, the user can only change the login password (the default login ID and password of the NAS are both "admin".)

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

3. The NAS Desktop will be displayed.

Migrating NAS

Users can migrate their existing NAS to another NAS model with all the data and configuration retained by simply installing all the hard drives of the original (source) NAS on the new (destination) NAS according to its original hard drive order and restart the NAS.

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

Topics covered in this chapter:
1. NAS models that support system Migration
2. NAS models that DO NOT support system migration
3. Disk Volumes Supported for System Migration
4. Migrating your NAS

NAS Models that Support System Migration

Before migrating to the destination NAS, make sure both the source and destination NAS models are powered off. NAS models that support system migration are listed below.

Source NAS		Destination NAS		Firmware Upgrade Required
Model	Firmware Version	Model	Firmware Version	
TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210	3.8 4.0.x 4.1.x and later	TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210	3.8.x and older 4.0.2	No
		TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U, TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U		
		TS-x28, TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.0.5 4.1.x and later	
		TVS-x63, TS-563, TS-x63U,		

		TS-x69, TS-x70, TVS-x71, TS-x79, TS-x80, TVS-x80, TS-x80U, TVS-x82, TVS-X82T		
TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U	3.8 4.0.x 4.1.x and later	TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210	3.8.x and older 4.0.2	Yes
		TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U, TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U		No
		TS-x28, TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.0.5 4.1.x and later	
		TVS-x63, TS-563, TS-x63U, TS-x69, TS-x70, TS-x70U, TVS-x71, TVS-x71U, TS-x79, TS-x80, TVS-x80, TS-x80U, TVS-x82, TVS-X82T	4.0.x 4.1.x and later	
TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53, TS-x53S Pro	4.1.x and later	TS-431U, HS-251, TS-x51/x51+, TS-x53, SS-x53	4.0.5 4.1.x and later	No
		TVS-x63, TS-563, TS-x63U, TS-x70, TS-x70U, TVS-x71, TVS-x71U, TS-x79, TS-x80, TVS-x80, TS-x80U, TVS-x82, TVS-X82T		
TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U, TS-x80, TS-x80U, TVS-x80, TVS-x82, TVS-X82T	3.8.x and older 4.0.2	TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210	3.8.x and older 4.0.2	No
		TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U, TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U		
		TS-x28, TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.0.5 4.1.x and later	
		TS-x69, TS-x70, TS-x79, TS-x80,	4.0.5	

		TS-x80U, TVS-x82, TVS-X82T		
	4.0.5 4.1.x and later	TVS-x63, TS-563, TS-x63U, TS-x69, TS-x69U, TS-x70, TS-x70U, TVS-x71, TVS-x71U, TS-x79, TS-x79U, TS-x80, TS-x80U, TVS-ECx80, TVS-x82, TVS-X82T	4.0.5 4.1.x and later	
		HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.1.2 and later	
TS-x31+	4.1.1	TVS-x71, TVS-x63, TS-563, TS-x63U, TS-x53, TS-x51/x51+, x31+	4.1.1	No
	4.1.2/4.1.3 and later	TS-x80, TVS-x80, TVS-x71U, TVS-x71, TVS-x63, TS-563, TS-x53, TS-x51/x51+, TS-x28, TS-x31+, TVS-x82, TVS-X82T	4.1.2/4.1.3 and later	No
HS-251/251+, TS-x51/x51+	4.1.1	TVS-x71, TVS-x63, TS-563, TS-x63U, TS-x53	4.1.1	No
	4.1.2/4.1.3 and later	TS-x80, TVS-x80, TVS-x71U, TVS-x71, TVS-x63, TS-563, TS-x63U, TS-x53, TS-x51/x51+, TVS-x82, TVS-X82T,	4.1.2/4.1.3 and later	No
TS-x53U, TS-x53 Pro/x53A, IS-453S, TS-x53S Pro	4.1.1	TVS-x71, TVS-x63, TS-563, TS-x63U, TS-x51/x51+	4.1.1	No
	4.1.2/4.1.3 and later	TS-x80, TVS-x80, TS-x71U,TVS-x71, TVS-x63, TS-x53, TS-x51/x51+, TVS-x82, TVS-X82T	4.1.2/4.1.3 and later	No
TVS-x63, TS-563, TS-x63U	4.1.2/4.1.3 and later	TS-x80, TVS-x80, TVS-x71U, TVS-x71, TVS-x63, TS-x53, TS-x51/x51+, TVS-x82, TVS-X82T	4.1.2/4.1.3 and later	No

	4.1.1	TVS-x63, TS-563, TS-x63U	4.1.1	No
TVS-x71	4.1.2/4.1.3 and later	TS-x80, TVS-x80, TS-x71U, TVS-x71, TVS-x63, TS-x53, TS-x51/x51+, TVS-x82, TVS-X82T	4.1.2/4.1.3 and later	No
TVS-x71U	4.1.1	TVS-x82, TVS-X82T, TS-x80, TVS-x80, TVS-x71U, TVS-x71, TVS-x63, TS-563, TS-x63U, TS-x69, TS-x79, TS-x70	4.1.1	No
	4.1.2/4.1.3 and later	TVS-x82, TVS-X82T, TS-x80, TVS-x80, TVS-x71U, TVS- x71, TVS-x63, TS-563, TS-x63U, TS-x53, TS-x51/x51+	4.1.2/4.1.3 and later	No
TS-x28	4.2.0 and later	TS-x28, TS-x31+/x31P/x31X/x31XU/1635, HS-251/251+, TS-x51/x51+/x51A, TS-x53/x53A, SS-x53, TVS-x63, TS-563, TS-x63U, TS-x69, TS-x69U, TS-x70, TS-x70U, TVS-x71, TVS-x71U, TS-x79, TS-x79U, TS-x80, TS-x80U, TVS-ECx80, TVS-x82, TVS-X82T	4.1.x and later	No

NAS Models that DO NOT Support System Migration

NAS models that do not support direct migration are listed in the below table. For these NAS models, first initialize the destination NAS and copy your data from the source NAS to the destination NAS (refer to the RTRR or Rsync chapter for details on data backup and replication.)

Source NAS		Destination NAS	
Model	**Firmware Version**	**Model**	**Firmware Version**
TS-x28, TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.1.x and later	TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210, TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U, TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U	3.8.x and older 4.0.2
TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U	4.0.5 4.1.x	TS-x10, TS-x12, TS-x19, TS-x20, TS-x21, HS-210, TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x59U, TS-x69, TS-x69U, TS-x70, TS-x70U, TS-x79, TS-x79U	3.8.x and older 4.0.2
		TS-x28, TS-x31/x31+, TS-431U, HS-251/251+, TS-x51/x51+, TS-x53, SS-x53	4.0.5 4.1.1 and older
TS-x28, TS-x31+/x51/x53	4.1.2 and later	TS-x31	4.1.x

- Download Station, iTunes Server, DLNA Media Server, and some multimedia features will be removed after migrating non-TS-x79/80/82/89 models to TS-x70U/TS-x79/80/82/85/89 models. The shared folders Multimedia/Qmultimedia, Download/Qdownload and all the downloaded files will be retained.
- The registered myQNAPcloud name on the source NAS will not be moved to the destination NAS after system migration. To use the same myQNAPcloud name on the destination NAS, change the myQNAPcloud name on the source NAS before system migration and register the same name on the destination NAS after the process is completed. Contact the QNAP technical support department if you encounter any issues during this process.

Disk Volumes Supported for System Migration

Refer to the following table for the relationship between the number of NAS bays and the disk volume supported for system migration.

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

	4 to 8-drive RAID 6,
	4-drive, 6-drive, or 8-drive RAID 10.

Migrating your NAS

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

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

Some system settings will be removed after system migration due to a different system design. Configure the following settings again on the new NAS:
- Windows AD
- Some Apps will need to be reinstalled.

QTS Basics and Desktop

QTS is a user-friendly NAS operating system designed to enhance every aspect of your NAS experience. With basic methods such as drag-and-drop or point and click, you can complete most NAS operations. Check the following links to learn more about QTS:

- Introducing QTS
- Using QTS Desktop

Introducing QTS

Built on a Linux foundation, QTS is shaped from an optimized kernel to deliver high-performance services that satisfy needs for file storage, management, backup, multimedia applications, surveillance, and more. The intuitive, multi-window and multi-tasking QTS GUI make it incredibly easy to manage your NAS, use its rich home applications, enjoy multimedia, and install more applications from an integrated App Center. QTS also adds value to business applications and effectively increase business efficiency with abundant features, including file sharing, iSCSI, virtualization, backup, privilege settings, and more. Coupled with various utilities and smart mobile apps, QTS is the ultimate platform for building a personal or private cloud, synchronizing data and sharing files.

NAS for Home - Easily enrich home entertainment and content sharing

Tons of photos, music, videos and documents are often scattered across multiple computers in modern homes. QNAP NAS feature plenty of handy applications to let you smartly connect and manage your data and enjoy a truly digital life in a well-secured home network. No boundaries for multimedia sharing at home, and no boundaries for sharing content with family, and friends. Learn more about the exciting features that a QNAP NAS offers you:

- Intuitive GUI with Multi-Windows, Multi-Tasking, Multi-Application, Multi-Device access support
- Cross platform data storage, backup and sharing center
- Revolutionary music, photo and home video center
- Personal cloud storage
- Free and large capacity for Dropbox-style data sync
- Hundreds of install-on-demand applications from the App Center
- Energy-efficient & eco-friendly

NAS for Business - Efficiently optimize business IT infrastructure

IT efficiency, coupled with low total cost of ownership (TCO) is an essential factor for business competitiveness. QNAP NAS features advanced capabilities for keeping businesses running at maximum efficiency including business-critical applications, seamless file sharing, easy integration into existing networks, flexible virtualized IT environments, and more. Learn more about the compelling features that a QNAP NAS offers your business:

- Large data storage, backup and file sharing center
- Supports both scale-up and scale-out solutions for growing data needs
- Advanced storage management with dynamic thin-provisioning, SSD caching and JBOD expansion functions
- Trustworthy data security and data encryption
- Reliable IP SAN storage (iSCSI) as primary and secondary storage for virtualization environments
- Private cloud storage
- Free and large capacity for Dropbox-style data sync
- Hundreds of install-on-demand applications from the App Center
- Development Center for third-party partners to build apps for the NAS

Using QTS Desktop

After you finish the basic setup and login to the NAS, the desktop will appear. Each main desktop feature is introduced in the following sections.

Topics covered in this chapter:

- QTS Desktop
- 2-step Verification

QTS Desktop

No.	Name	Description
1	Show Desktop	Minimize or restore all open windows.
2	Main Menu	Show the Main Menu. It includes two parts: 1) SYSTEMS: Key system features and options designed to help you manage or optimize your NAS. 2) APPLICATIONS: Applications developed by QNAP to enhance your NAS

		experience. Please note that the default Internet browser, instead of a new window on the NAS Desktop, will be launched once you click a third-party application.
3	Search	Enter keywords in the search bar to find an application or function and related instructions. Click the search result to launch an application or function or consult its online QTS help.
4	Background Task	Review or control (such as pause or postpone) all the tasks running in the background. For example, HDD S.M.A.R.T. scanning, anti-virus scanning, file backup, or multimedia conversion.
5	External Device	List all external storage devices and USB printers that are connected to the NAS via its USB or SATA ports. Click a listed device to open File Station to view this device. Click "More>>" to open the External Device page for relevant settings and operations (for more information about File Station, refer to the File Station chapter). Click the eject icon (up-arrow icon) to eject the external device.
6	Notification and Alert	You can check recent errors, warnings, and notifications here. Click "Clear All" to clear the list. To view all historical events, click "More>>" to open System Logs. For more information about System Logs, refer to the System Logs chapter.

7	Options	• Profile: Specify your email address and change your profile picture. You can also check System Logs and edit the Login Screen here.
		• Wallpaper: Change the default wallpaper or upload your own photo and set it as the wallpaper.
		• 2-step Verification: Enable 2-step Verification to enhance the security of user accounts. For more information, refer to the 2-step Verification section.
		• Change Password: Change your login password.
		• E-mail Account: Set up the email address you use when sharing files via email in Music Station, Photo Station, Video Station, or File Station.
		• Miscellaneous:
		  o Auto log-out after an idle period of: Specify the idle period after which the user will be automatically logged out.
		  o Warn me when leaving QTS: Users will be prompted for confirmation every time they try to leave the QTS Desktop (such as closing the browser or clicking the "back" button of the browser). It is recommended to enable this option.
		  o Reopen windows when logging back into QTS: If you enable this option,

all the current desktop settings (such as "the windows opened when your log out") will be retained until your next login.

o Show the desktop switching button: Check this option to hide the next desktop button (No. 12) and only display them when you move your mouse cursor close to the buttons.

o Show the desktop switching button: Enable this option to show the "next desktop" button (No. 12). If you disable this option, the "next desktop" button will only appear when you move the mouse cursor near it.

o Show the link bar on the desktop: Enable this option to show the link bar (No. 13, No. 14, No. 15, and no.16).

o Show the Dashboard button: Enable this option to show the Dashboard button (NO. 10).

o Show the NAS time on the desktop: Enable this option to display the NAS time in the bottom-right corner of the desktop.

o Keep Main Menu open after selection: Keep the Main Menu pinned/unpinned on the desktop.

o Show a list of actions when external storage devices are detected: Enable this option and the Autoplay dialog box will appear after you plug in an external device.

8	Admin Options	Configure user-specific settings, change your user password, restart/shut down the NAS or log out.

Configure user-specific settings, change your user password, restart/shut down the NAS or log out.

- Last login time: The last time when you logged in to the system.
- Options: Refer to the previous section.
- Sleep: Put your NAS into sleep. There are three ways to wake up the NAS: 1) Press the power button until you hear a beep; 2) Use the Wake-on-LAN (WOL) feature with QNAP Qfinder Pro or Qmanager. Note that to use this method, WOL must be enabled in "Control Panel" > "Power" > "Wake-on-LAN(WOL)"; 3) Press the power button on a RM-IR002 or MCE remote control.
  o **Note: This feature is only available on certain models.**
- Restart: Restart your NAS.
- Shutdown: Shut down your NAS.
  o **Note: To power off a NAS, you can also:**
    ▪ **Press and hold the power button on your NAS for 1.5 seconds.**
    ▪ **Run Qfinder Pro and click "Tools" > "Shut down Server".**
- Logout: Log yourself out

9	More	• Help: Show NAS references, including Quick Start, Virtualization Guide, Help Center, and Tutorials.
		• Language: Choose your preferred language.
		• Desktop Preference: Applications can be opened in Tab Mode, Window Mode, or Frameless Mode. Only Tab Mode is available if you log in to the NAS using a mobile device.
		◦ Tab Mode: In this mode, the application window will be expanded to fit the entire NAS Desktop, and only one application window can be displayed at a time.
		◦ Window mode: In this mode, the application window can be resized to your preferred shape.
		◦ Frameless Mode: In this mode, applications will be opened without their frames.
		• Help Request: Send a help request to QNAP.
		• About: Check the NAS model, firmware version, numbers of hard drives already installed and empty bays, used and unused storage space.
10	Dashboard	Check important NAS statistics, including system and hard drive health, resources, storage usage, online users, scheduled tasks, etc. Click the header in each widget to open its own page.
11	Desktop Area	Arrange or remove the applications on the desktop.
12	Next Desktop/ Last Desktop	Switch between different desktop pages.
13	myQNAPcloud	Go to the myQNAPcloud website.
14	QNAP Utility	Check and download NAS utilities and mobile apps.
15	Feedback	Go to QNAP Wiki or QNAP Forum, or seek Customer Service.
16	Help Request	Send a help request to QNAP.
17	Network Recycle Bin	All of the deleted items can be found here. Right click on this icon to open the Network Recycle Bin, empty it (delete files permanently), or configure it (refer to the Network Recycle Bin chapter for more information.)

2-step Verification

2-step Verification enhances the security of user accounts. Once enabled, you will need to enter a one-time security code (6 digits) in addition to your password whenever you sign in to the NAS. 2-step verification requires a mobile device with an authenticator app which supports the Time-based One-Time password (TOTP) protocol. Supported apps include Google Authenticator (Android/iPhone/BlackBerry) or Authenticator (Windows Phone.)

Start 2-step verification
1. Install the authenticator App on your mobile device: For Android and iOS devices, install the Google Authenticator App from their respective App stores. For Windows Phone, install the Authenticator from its Store.
2. The system times of your mobile device and NAS must be synchronized. It is recommended to use the time provided from the Internet.
3. Go to "Options" > "2-step Verification" and click "Get Started". Complete the steps in the wizard to set up the NAS and your mobile device.
4. Configure your authenticator App by scanning the QR code or by entering the Secret Key into the App.
5. Enter the code generated from the app to the NAS to verify the correct configuration.
6. Select an alternative verification method by emailing you a security code or by answering a security question if you cannot use your mobile device. To email a security code, the SMTP server must be properly configured in "Control Panel" > "Notification" > "E-mail".

Sign in QTS with 2-step verification
After your username and password are verified, you will be promoted to enter a security code. Enter the code currently provided from the authenticator app to sign in to QTS. If you cannot use your mobile device or your device is lost, you can select "Verify another way" to sign in with your chosen alternative verification method.

Stop 2-step verification
If you want to disable 2-step verification, go to "Options" > "2-step Verification" and click "Stop". Administrators can disable 2-step verification for other NAS account users if they are locked out by going to "Control Panel" > "Users" > "Edit Account Profile"

If an administrator cannot use a mobile device to sign in to QTS and no other administrators are available to disable 2-step verification for the locked-out administrator, the NAS must be restored to factory settings by physically pressing the "RESET" button on the NAS.

> **Tip:**

- All of the Dashboard widgets can be dragged onto the desktop for monitoring specific details.
- The Dashboard will be presented differently on different screen resolutions.
- The color of the Dashboard button will change based on the status of system health for quick recognition.

Note:
- The recommended minimum screen resolution for QTS 4.x is 1024x768.
- The sleep function will automatically be disabled if the NAS has QNAP expansion enclosure(s) connected to it.

System Settings

Go to "Control Panel" > "System Settings" to set up your NAS.
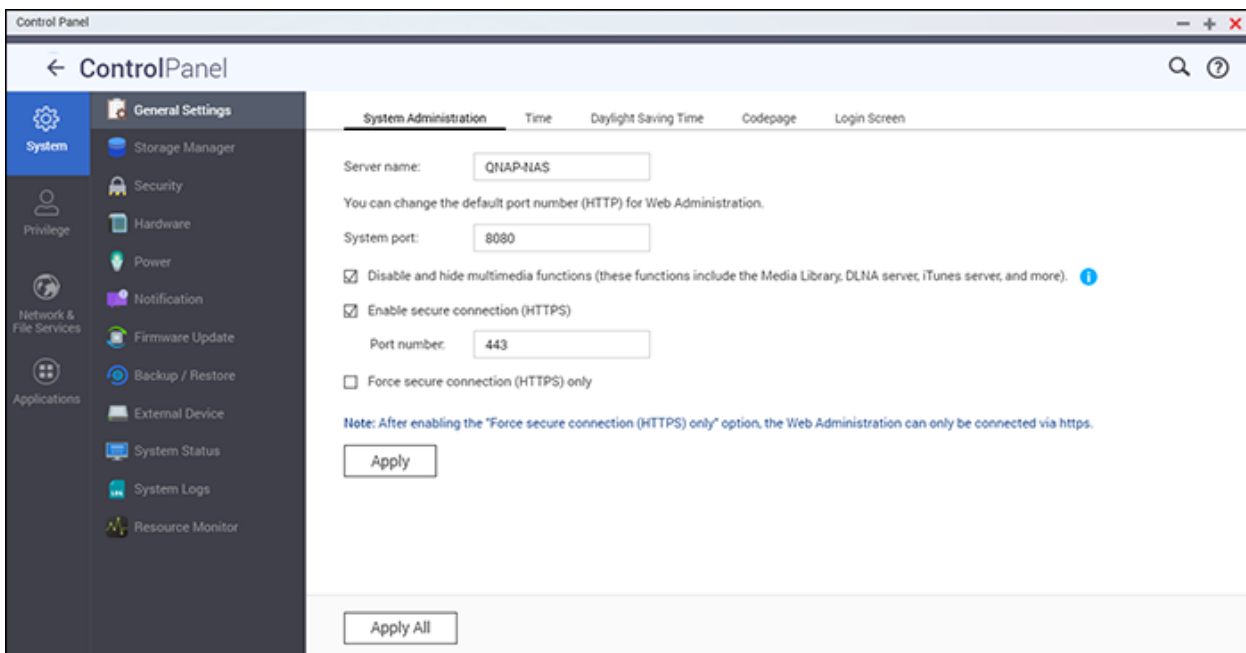
For details on the settings, refer to the following links:

- General Settings
- Storage Manager
- Network
- Security
- Hardware
- Power
- Notification
- Firmware Update
- Backup/Restore
- External Device
- System Status
- System Logs

General Settings

Go to "Control Panel" > "System Settings" > "General Settings" to configure basic settings of the NAS.
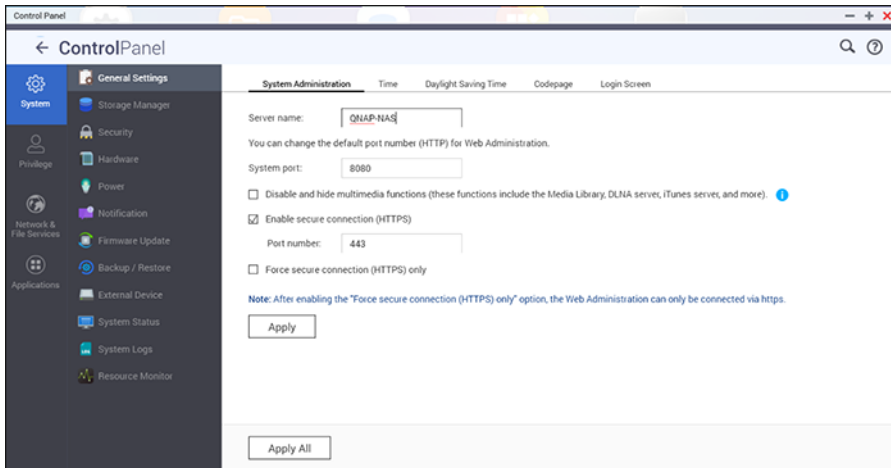
Topics covered in this chapter:

- System Administration
- Time
- Daylight Saving Time
- Codepage
- Login Screen

System Administration

- **Basic Settings:** Enter the name of the NAS. The NAS name supports maximum 14 characters and can be a combination of letters (a-z, A-Z), numbers (0-9), and dash (-), Space ( ), period (.), or pure numbers are not allowed. Enter a port number for system management. The default port is 8080. The services which use this port include: System Management, Photo Station, Music Station, File Station and Download Station. If you are not sure about this setting, use the default port number.
- **Enable Secure Connection (HTTPS):** Allows users to connect to the NAS by HTTPS. Enable secure connection (HTTPS) and enter the port number. If the option "Force secure connection (HTTPS) only" is enabled, users can only connect to the web administration page by HTTPS.
- **Force Secure Connection (HTTPS):** After enabling this option, you can only connect and log into the NAS using HTTPS.

- **Disable and hide the home/multimedia features such as Photo Station, Music Station, Surveillance Station, Download Station, iTunes server, and DLNA media server:** Multimedia features, including Photo Station, Music Station, Video Station (both 2.0 and 1.0.5), Surveillance Station, Download Station, DJ Station, iTunes server, Media Library and DLNA media server, may be hidden or disabled by default on the following NAS models: x70U, x79 Pro, x79U, TS-x51,TS-x31+, TS-x31,TS-269H and HS-210. To enable the multimedia features for those models, uncheck this option.

Time

- **Basic time settings:** Adjust the date and time format and time zone according to the location of the NAS. If the settings are incorrect, the following problems may occur:
  - When using a web browser to connect to the NAS or save a file, the displayed time of the action will be incorrect.
  - The time of event logs will be inconsistent with the actual time when an action occurs.
  - All scheduled jobs will be run at an incorrect time.
- **Manual Setting:** Select this option to manually set the time of the NAS.
- **Synchronize with an Internet time server automatically:** Enable this option to automatically synchronize the date and time of the NAS with an NTP (Network Time Protocol) server. Enter the IP address/domain name of the NTP server (for example: time.nist.gov, time.windows.com) then enter the time interval for synchronization. This option can only be used when the NAS is connected to the Internet.
- **Set the server time the same as your computer time:** To synchronize the time of the NAS with your computer's time, click "Update" next to this option.

> **Note:** First time synchronization may take several minutes to complete.

Daylight Saving Time

If your region uses daylight saving time (DST), enable "Adjust system clock automatically for daylight saving time" and click "Apply". The latest DST schedule of the time zone specified in the "Time" section will be shown. The system time will be adjusted automatically according to the DST. Note that if your region does not adopt DST, the options on this page will not be available. To manually enter the DST table, select the option "Enable customized daylight saving time table". Click "Add Daylight Saving Time Data", enter the daylight saving time schedule, and click "Apply" to save the settings.

Codepage

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

> **Note:** All of the files and directories on the NAS use Unicode encoding. If your FTP clients or PC OS does not support Unicode, select the language which is the same as the OS language in order to properly view files and directories on the NAS.

Login Screen

The administrator can customize the login screen by going to "Control Panel" > "General Settings" > "Login Screen". There are two templates to choose from: classic and photo wall.

Classic login page settings:
- Show firmware version: Display QTS firmware verion on bottom right of login page.
- Show the link bar: Display links to myQNAPCloud, QNAP Utility, and Feedback links to the bottom of the login page.
- Background: Select a photo to use as login screen background, then select center, fill, fit, stretch, or tile as the display mode. Click remove to set background to default image.
- Logo: Select image to use as a logo on login screen. Click remove to remove logo.
- Message: Enter a personal login message. You may select font color and size.

Photo Wall page settings:
- Show firmware version: Display QTS firmware verion on bottom right of login page.
- Show the link bar: Display links to myQNAPCloud, QNAP Utility, and Feedback links at the bottom of the login page.
- Message Title: Enter a personal message title for the login page.
- Message: Enter a personal message for the login page.
- Randomly select 100 photos: Use 100 random photos stores on the NAS for login page background.
- Display the most recently shared 100 photos: Use 100 most recently shared photos on NAS for login page background.
- Change Picture: Select an image to use as a logo on login screen. Click remove to remove logo.
- Use my profile picture: Use user account profile picture as login screen logo.

After you finish the above settings, click "Preview" to preview your settings or "Apply" to save changes.

Storage Manager

Based on QNAP's Flexible Volume Architecture, the Storage Manager provides a secure, flexible and comprehensive approach to managing data on your NAS and offers useful features such as:

- Storage pools & multiple RAID groups
- Thin-provisioned volumes & space reclamation
- Snapshot & Snapshot Replica
- Online capacity expansion

These features provide a complete storage solution for your valuable data.
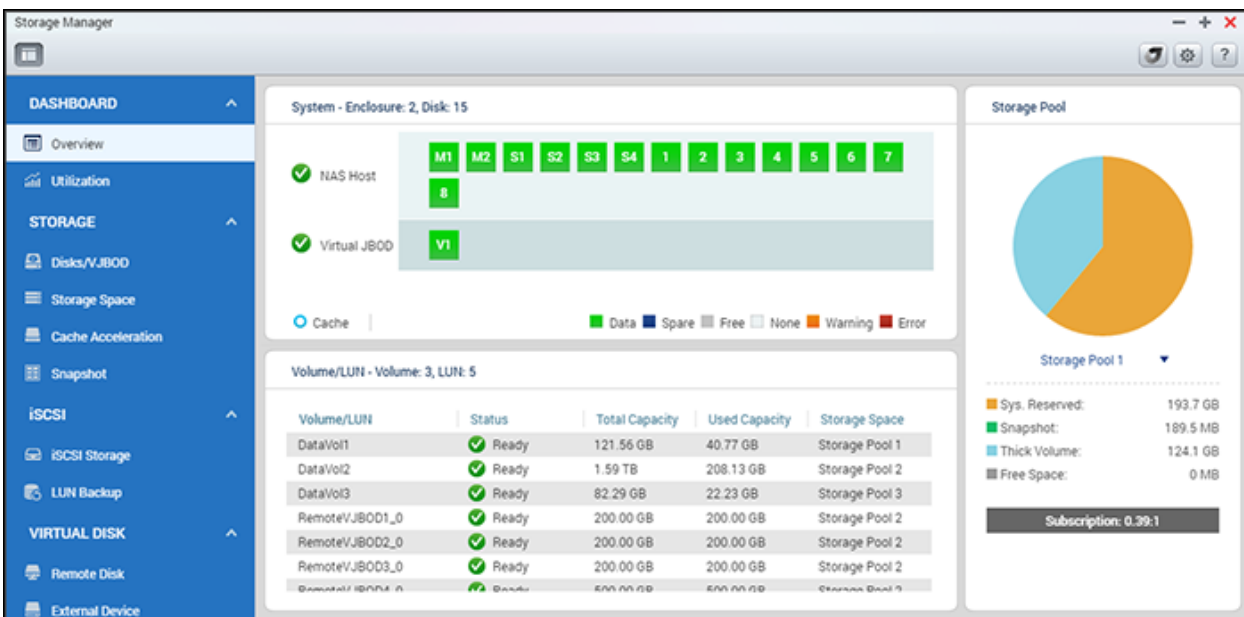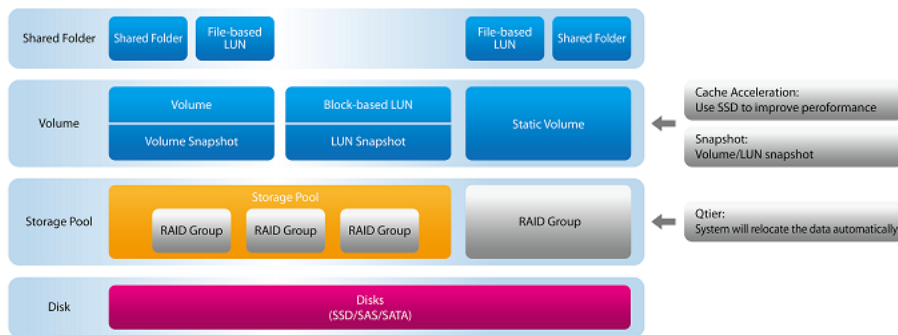

> **Note:** Some features listed above are only applicable to certain NAS models.

QNAP Flexible Volume Architecture

The QNAP Flexible Volume Architecture consists of the following four layers: Disk Management, Storage Pool Management, Volume Management and Shared Folder Management, as shown below:
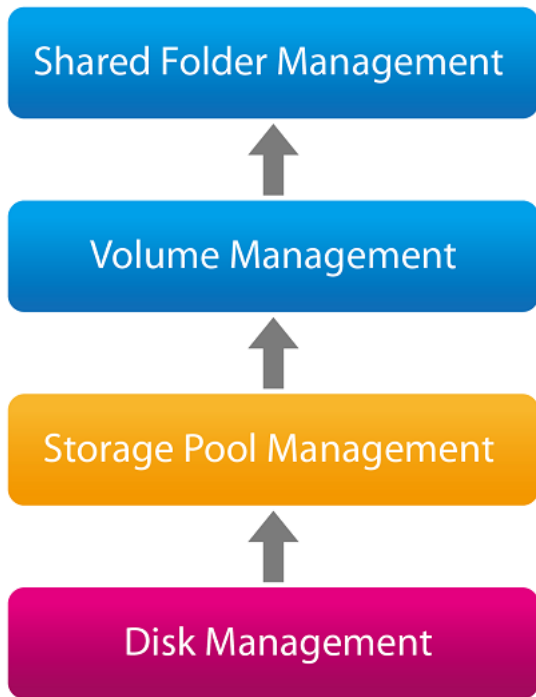
Basic Storage Management Architecture

Each layer is designed to cover an aspect of the storage system. The four layers combine to offer you a comprehensive range of options to store and protect your data on your QNAP NAS.

- **RAID Group:** RAID groups combine multiple physical disk drives into a single logical unit to provide data redundancy, performance improvements, or both.
- **Storage pool:** Storage pools aggregate physical hard drives or RAID groups into large storage spaces. A storage pool can be expanded by adding new RAID groups into it or by adding new disks to an existing RAID group.
- **Hot Spare:** A hot spare is a backup hard drive in the NAS that is used only when a disk in a RAID group fails.   The hot spare will automatically replace the faulty disk and the data will be rebuilt to the hot spare.

- **Volume:** Volumes are storage spaces on your NAS. A volume is formatted by the file system to store shared folders and files. There are three types of volumes: thick, thin and static. Thick/thin volumes must be created in a storage pool, and a storage pool can contain multiple thick/thin volumes. A thick/thin volume can be resized to a greater capacity if there is available space in the storage pool. Static volumes, on the other hand, are created from a RAID group instead of a storage pool. A static volume can be expanded by adding new RAID groups into it or by adding new disks to an existing RAID group. More information on volumes can be found [here](#).

- **iSCSI LUN:** iSCSI LUNs are logical volumes mapped to iSCSI targets. There are two types of LUNs: block-based and file-based. Block-based LUNs are usually preferred to File-based LUNs. The difference between block-based LUN and file-based LUN can be found [here](#).

- **Shared folder:** Shared folders are created in volumes and are used to store and share files with users or groups that have access privileges.

For more information on Storage Manager, please refer to the links below:
- [Creating new storage pools](#).
- [Creating new volumes](#).
- [Creating new shared folders](#).
- [Creating iSCSI LUNs](#).

Advanced Storage Architecture

Qtier - Auto-tiering storage management architecture
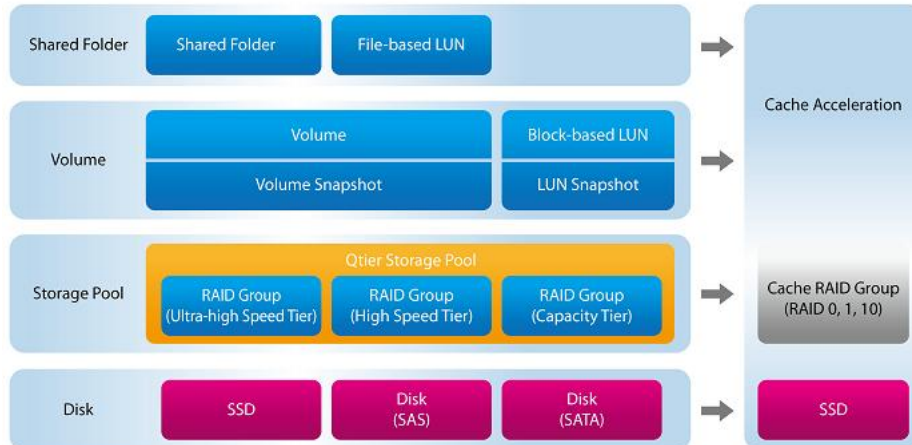
- Qtier storage pool: Qtier is an automated-tiering storage solution that consists of different types of disks to form a multiple-drive volume that during low-load times or based on your schedule:
  - Moves frequently used data onto high-performance disks (ie. SSDs) for high-availability or high I/O cache throughput.
  - Moves less frequently used data onto low-cost, high-capacity disks (ie. SATA drives) for better cost efficiency.
- There are three speed tiers of disks:
  - Ultra-High speed tier: Ultra-high speed tier is a RAID group that consists of SSD for hot data.

- o High speed tier: High speed tier is a RAID group that consists of SAS disks for the data that is between hot data and cold data.
  - o Capacity tier: Capacity tier is a RAID group that consists of SATA disks for cold data.
- Cache Acceleration: The Cache Acceleration feature is designed to boost access performance of the NAS by the use of SSD(s). More information on cache acceleration can be found here.

Click here for more information on setting up Qtier.

Disaster-recovery storage management architecture
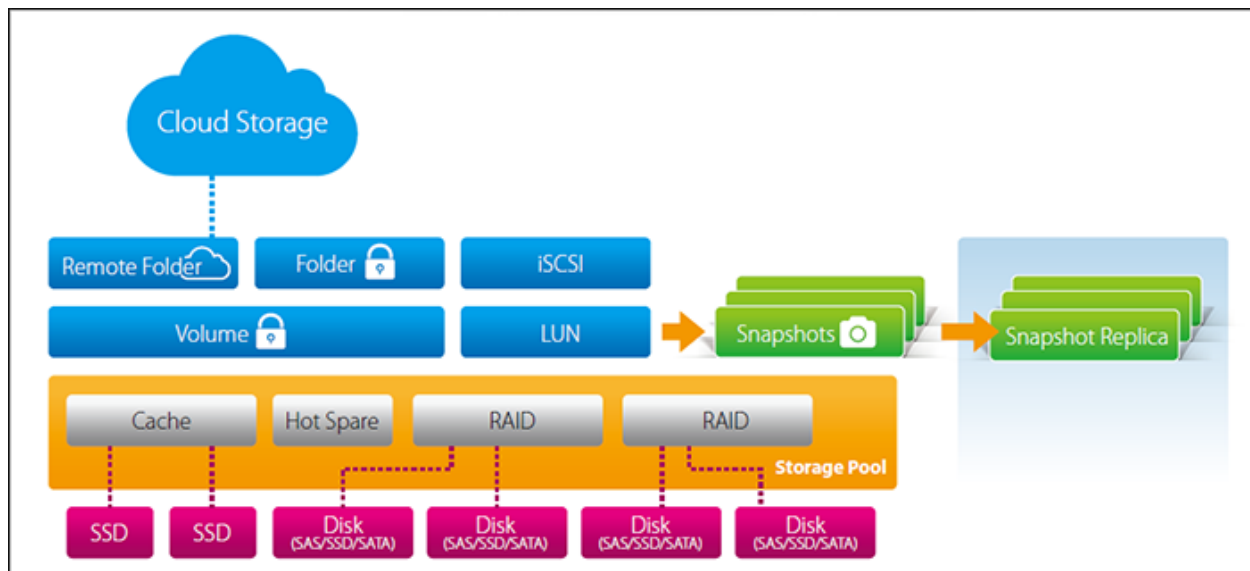
- Snapshot: Take a snapshot to record the state of a volume/LUN. After snapshots are taken, they can be used to restore the volume/LUN's state to the time the snapshot was taken. Users may also choose to only restore particular folders/files in the volume from the Snapshot.
- Snapshot Replica: The Snapshot Replica allows you to replicate the volume/LUNs between different remote servers using snapshot technology, which provides a flexible and efficient backup service for IT professionals.
- Snapshot Vault: Snapshot Vault stores snapshots sent from remote NAS via Snapshot Replica. Snapshot Vault also lets you manage and restore remote snapshots.

Click here for more information on creating replication jobs.

This architecture supports four distinct types of volumes adapted by QNAP over the years, and each volume type supports different storage features:

Features	Legacy Volume	Static Volume	QTS 4.1 Storage Pool Flexible Volume	QTS 4.2 Storage Pool Flexible Volume
Performance level	High	High	Medium	Medium
Online RAID migration	●	●	●	●
Online RAID expansion	●	●	●	●
File-based LUN	●	●	●	●
Block-based LUN			●	●
Thin provisioning			●	●
SSD cache		●	●	●
JBOD RAID expansion		●	●	●
JBOD expansion roaming		●	●	●
Snapshot				●
Snapshot Replica				●
Snapshot Vault				●

For specific setup of the Storage Manager, please refer to the following links:

- Dashboard
- Storage

- [iSCSI](#)
- [Virtual Disk](#)

Dashboard

The Storage Manager dashboard provides an overview for IT administrators to easily monitor and manage storage allocations.
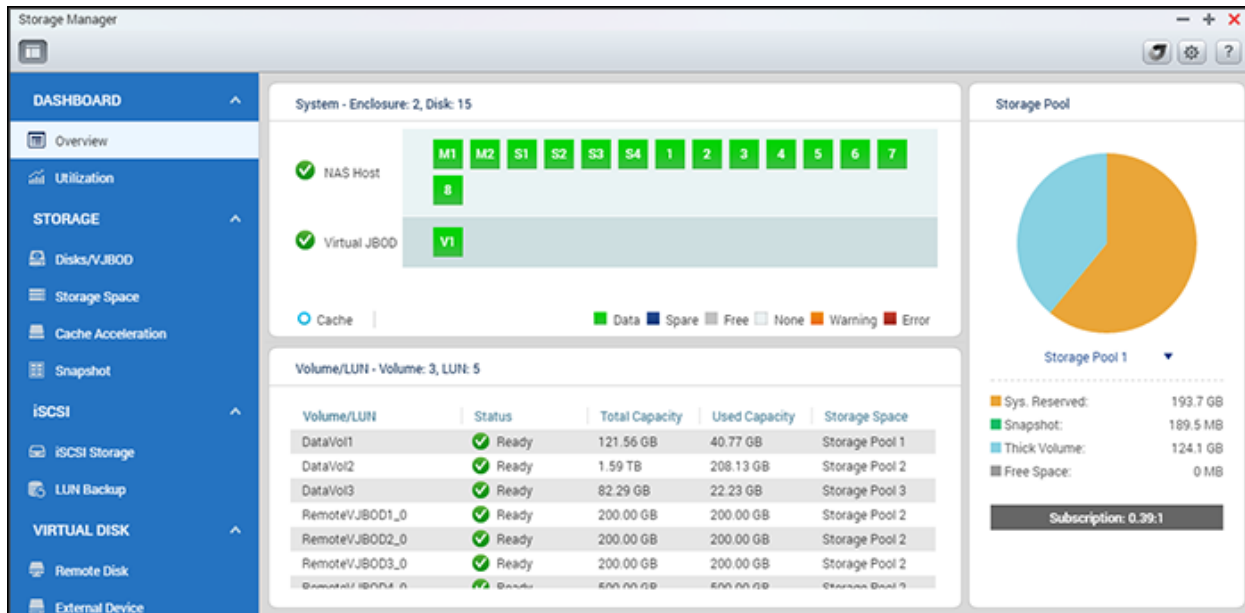
Overview

There are three sections on the page: Disk, Volume/LUN and Storage Pool. They are described below:

- Disk: The physical hard disk drives and their associated storage hosts (including both the NAS and its connected expansion enclosures) are shown in this section. Click the hard disk drive icon to bring up the Disk Health window. For details on the Disk Health window, please refer to the Disks chapter.
- Volume/LUN: All available logical volumes, their capacity and type (Volume, LUN and Unused) are listed in this section. For details on volumes and LUN, please refer to the Volumes chapter.
- Storage Pool: This section provides a space usage overview on the storage pool created on the NAS. You can check the space distribution on the pie chart for each storage pool (including the size of reserved system space, thick volume and free space) and its subscription. Subscription is the ratio between claimed space and available space in the storage pool. If a user creates a thin-provisioned volume with 10TB claimed space, while the available space is only 1TB, the "Subscription" value in the "Overview" page will be 10:1, meaning that the thin-provisioned space is oversubscribed and users must note that the available space in storage pool is too low. You can also click on the down arrow next to the storage pool to switch between storage pools. For details on storage pools, please refer to the Storage Pools chapter.

Utilization

This page is designed for users to monitor storage utilization of their NAS. With volume and storage pool usage information presented on this page, users can manage their storage system more effectively and spot potential issues based on trends over a period of time (from the last hour to the last year.)

Select to view the storage usage rate of a particular volume or storage pool and specify the period. Click "Clear Record" to reset the utilization graph.

Note: Utilization only applies to certain NAS models. To check for applicable models, please refer to the product comparison table on the QNAP website.

Storage

Manage volumes, storage pools, hard disk drives, snapshots, encrypt and decrypt file systems, and configure cache acceleration with Storage Manager.
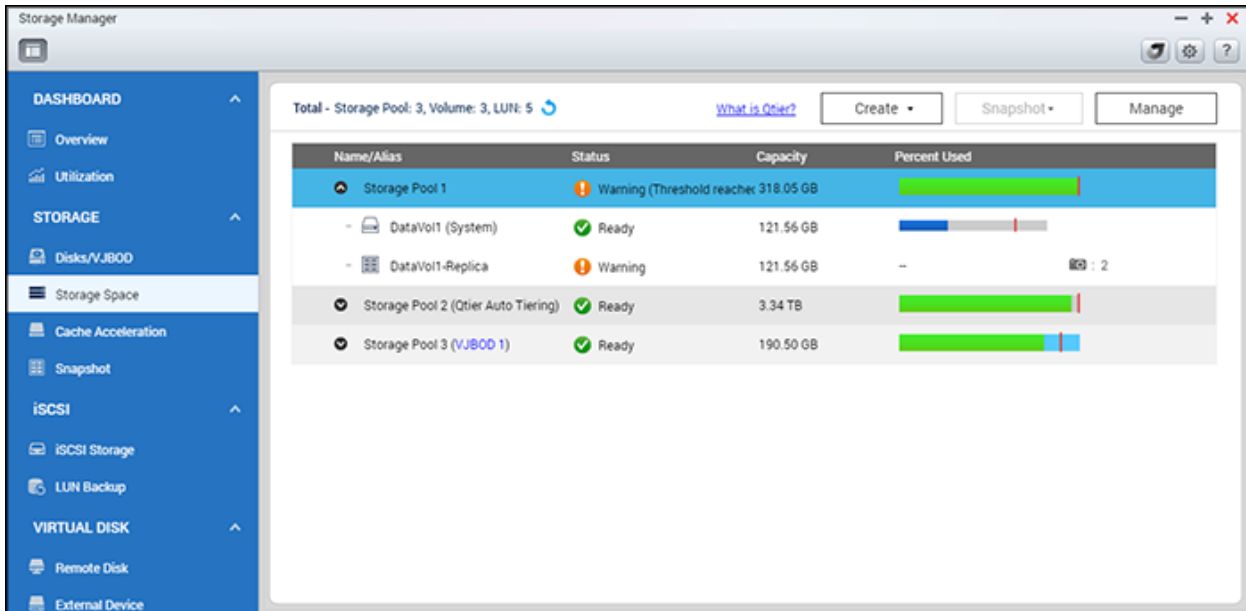
For details on the features, refer to the following links:

- Disks/JBOD
- Storage Space
- Cache Acceleration
- Snapshot
- Qtier (Auto Tiering)

Note: Some of the features listed above are applicable to certain models. Please check for applicable models first as you review descriptions of the features.

Disks/VJBOD

This page is designed for users to monitor and manage hard disk drives installed on the NAS and its connected expansion units (both expansion enclosures and VJBOD (also known as Virtual JBOD)). Users can quickly isolate and identify hard drives for relevant maintenance tasks.
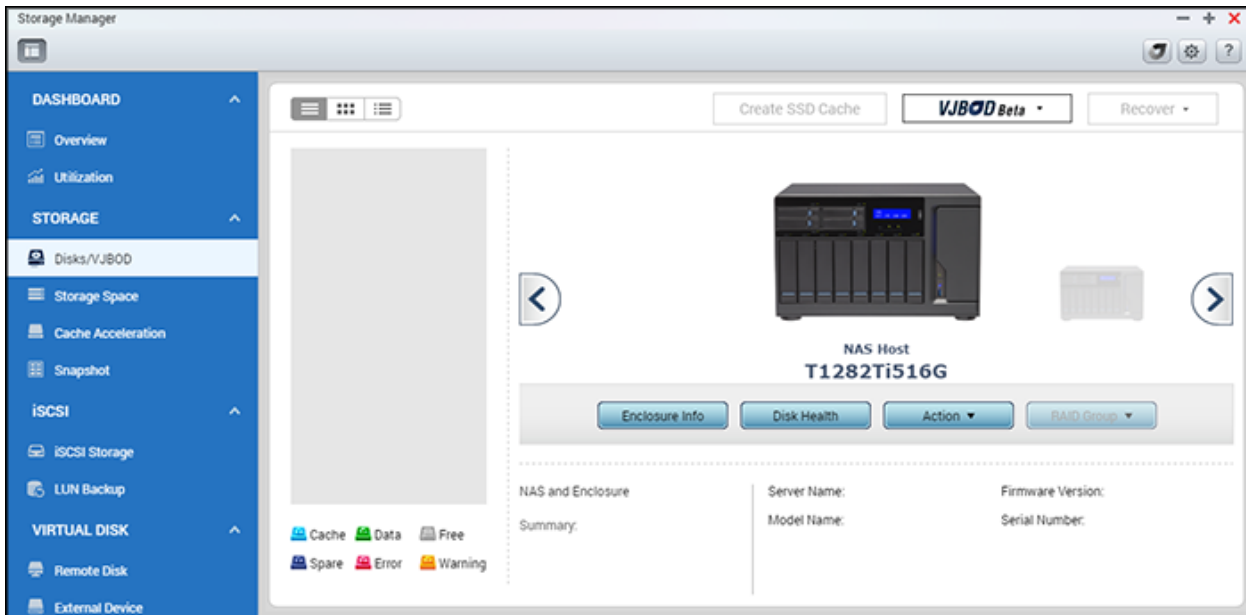
In this chapter, the following topics are covered:

- Disks
  - Managing NAS Hosts
  - Managing Disks
  - HDD S.M.A.R.T. Information
  - Disk Health Global Settings
- Expansion Enclosures
  - Managing Physical Expansion Enclosures
  - Recovering Physical Expansion Enclosures
  - Managing Virtual Expansion Enclosures (VJBOD)
    - Introducing VJBODs
    - Creating VJBODs with new iSCSI LUN (using Create Virtual JBOD's Disk Wizard)
    - Creating VJBODs with existing iSCSI LUN (using Create Virtual JBOD's Disk Wizard)
    - Using VJBODs
    - Managing and Monitoring VJBODs
    - Detaching and Reconnecting VJBODs
    - Data Roaming
    - Automatic Reconnection

Disks

> **Note:** Hot-plugging is not supported for M.2, PCIe, and mSATA drives.

Managing NAS Hosts

Click a NAS under "NAS Host" in the system component panel to check its general information. Refer to the following table for actions available to manage a NAS host:

Action	Description
Enclosure Info	Click this button to check details of an enclosure, including the model, serial number, firmware version, BUS type, BIOS version, CPU temperature, system temperature, power status, system fan speed and power fan speed.
Locate (under "Action")	Click this button and the chassis LEDs of the selected NAS host will blink for easy identification.
RAID Group	Click this button and select a RAID group to check its details, including capacity, RAID group name, RAID type and disk member.

> **Note:** You can click "NAS Host" in the system component panel and click "Action" > "Port Table" to check the port speeds.

Managing Disks

Click "+" beside the NAS host in the system component panel and select a disk to check its general information. The legend shown under the system component panel is provided to indicate the types of hard disk drives:

- Cache: A disk drive configured as cache.
- Data: A disk drive that contains data.
- Free: An empty disk drive that does not have any data on it.
- Spare: A disk drive configured as spare drive for a RAID group.
- Error: A disk drive detected with errors (could be bad sectors or I/O errors) and it is recommended that this disk drive is to be replaced immediately.
- Warning: A disk drive is approaching failure.

Refer to the following table for actions available to manage a disk:

Action	Description
Disk Info	Click this button to check details of a disk, including the model, model number, serial number, capacity, firmware version, ATA version and ATA standard.
Disk Health	Click this button to check disk S.M.A.R.T information. More details about S.M.A.R.T information will be provided in the next table.
Scan Now (under "Action")	Click this button to scan the disk for bad blocks. If bad blocks are found, the number of bad blocks will be displayed in the "Status" field. Check the bad block sectors by clicking on the "bad blocks" message so long as the disk is not busy. You can also use this function if a drive is in an error state. In this case, if no bad blocks found after a complete scan, the error state of drive will be changed back to normal.
Locate (under "Action")	Click this button to locate drives using LED lights for easy identification of physical hard drives.
Set as Enclosure Spare (under "Action")	Click this button to set the chosen hard disk drive as an enclosure spare drive in RAID 1, RAID 5, RAID 6, or RAID 10. In case a spare drive is shared by multiple RAID groups, that spare drive will be used to replace the first failed drive across all RAID groups. Please note that the capacity of the enclosure spare drive must be equal to or larger than that of the member drive in a RAID group and this option is only available for an empty disks. Note that an enclosure spare can only be used within an enclosure.
Disable Spare (under "Action")	Click this button to cancel the chosen hard disk drive as an enclosure spare drive.
New Volume (under "Action")	Click this button to create a new volume. For details, please refer to the chapter on Volumes.
RAID Group	Click this button and select a RAID group and check its details, including capacity, RAID group name, RAID type and disk member.
View Mode (located above the system component panel)	Switch to list view using the list view icon on top-left of the page. In the list view, you can show or filter for disks. Set the filter from the drop down list to only show hard disks based on the device (enclosure or NAS they belong to), model, type (HDD or SSD), BUS type, capacity, used type (data, free, error, spare, cache, or none) and status. Click "Refresh" to refresh the list. You can also perform sequential read and IOPS read tests (under "Performance

	test"), schedule weekly sequential read tests, and check the test results to gauge the performance of the tested disks.

HDD S.M.A.R.T Information

Switch to the icon view (or tree view) and click the "Disk Health" button to bring up the Disk Health window.

First select the NAS Host or an expansion enclosure and one of its disks to check for S.M.A.R.T information. Refer to the below table for descriptions of each field:

Field	Description
Summary	This page provides an overview on hard disk S.M.A.R.T details and the result of the latest test.
Hard Disk Information	This page shows hard disk details, including disk model, model number, serial number, disk capacity, firmware version, ATA version and ATA standard.
SMART Information	This page shows the results of the latest S.M.A.R.T test.
Test	Click on this tab to choose a rapid or complete S.M.A.R.T testing method for the hard disks. The test result will be shown.
Settings	Configure the following settings on this page: 1) Enable Temperature Alarm: enable this option to set the temperature alarm. When the hard disk temperature exceeds the specified threshold level, the system will record an error message; and 2) Rapid and complete test schedules: schedule a rapid or complete test here. The result of the latest test can be viewed on the "Summary" page. Click "APPLY to Selected HDD" to apply the settings configured on this page only to the selected hard disk drive or "APPLY to All HDDs" to all hard disk drives.

Disk Health Global Settings

You can enable the following Disk Health settings in the Global Setting dialog window (the "setting" icon next to "?" on top right side of the screen):

- Activate Predictive SMART Migration: With Predictive SMART Migration, a warning message will pop up when an S.M.A.R.T error is detected on a hard disk drive (indicating that the RAID group that the hard drive disk belongs to is likely to fail very soon.) The migration sequence will be initiated for that RAID group to ensure the availability of that RAID group. The data from the disk with errors will be migrated to a healthy spare drive. The migration process is much faster than the standard rebuilding process.
- Disk S.M.A.R.T polling time (minutes): This value is the interval the hard drive disks are scanned for S.M.A.R.T errors and the default is 10 minutes.

- TLER/ERC timer (seconds): This option allows system administrators to configure the hard disk drive R/W response time. If you are not sure about the interval to set for the timer, please leave it as is.

Expansion Enclosures

Expansion enclosures are designed for expanding the storage capacity of a QNAP NAS. This is achieved either through a direct, physical connection between a NAS and expansion enclosures (via USB or mini-SAS cables) or a network connection between two NAS (using a LAN connection).

Managing Physical Expansion Enclosures

> **Note:** The function or its content is only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website.

First click an expansion enclosure (REXP) in the system component panel to check its general information. Refer to the following table for actions available to manage an expansion enclosure:

Action	Description
Enclosure Info	Click this button to check on details of the chosen enclosure, including the enclosure model, serial number, firmware version, BUS type, CPU temperature, system temperature, power status, system fan speed and power fan speed.
Locate (under "Action")	Click this button and the chassis LEDs of the selected expansion enclosure will blink for easy identification.
Safely Detach (under "Action")	Click this button to safely remove the enclosure from its host.
Update firmware (under "Action")	Click this button to update firmware for the chosen enclosure.
Rename enclosure (under "Action")	Click this button to rename the chosen enclosure.
RAID Group	Click this button and select a RAID group to check its details, including capacity, RAID group name, RAID type and disk member.

Recovering Physical Expansion Enclosures

> **Note:** The function or its content is only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website.

Click "Recover" on the top-right side of the window, and there are three options available:

1. Recover Enclosure: Recover volumes on an enclosure that was accidentally disconnected (e.g. unscheduled shutdown or unplugged SAS cable) from the NAS host. When this occurs, a broken chain symbol will be shown in the Chassis View and the status of the affected storage pool will be shown as "Error" and RAID group as "Not active".

2. Reinitialize enclosure ID: This is only used to reorder ID for expansion enclosures in a numerical manner.

3. Scan All Free Drives: Scan drives in a free state in the NAS and attached enclosures for existing volumes or storage pools.

> **Note:** The "Recover" button is only available if the disconnected expansion enclosure contains volumes.

Managing Virtual Expansion Enclosures (VJBOD)

Introducing VJBODs

Virtual JBOD allows you to allocate the free space of a QNAP NAS to another NAS in order to maximize the total available storage capacity for that NAS. The following figure illustrates how Virtual JBOD works. An iSCSI LUN on a remote NAS is created and added to a local host (host NAS in this example) as a hard drive to expand the Storage Space on the host NAS.
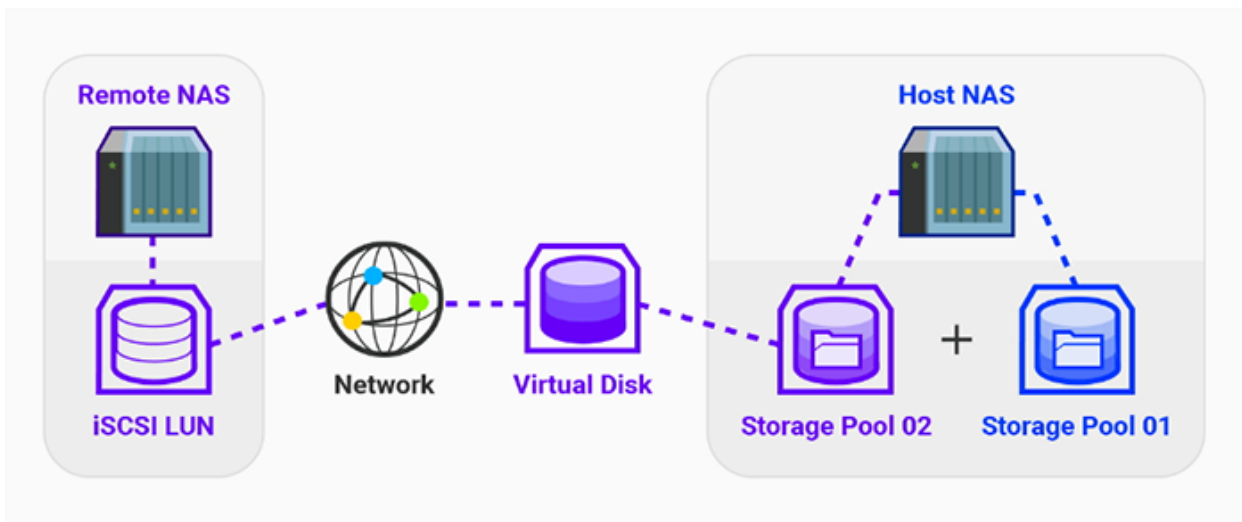
> **Note:**
> - This function or its content is only applicable to some models (refer to the software specification page on the QNAP website for further details) and requires firmware 4.2.2 (or newer).
> - Any QNAP NAS that supports iSCSI and storage pools can be used as a remote NAS, but it is recommended that they use firmware 4.2.1 (or newer) and have at least 154GB free space.
> - For greater connection stability and to automatically recover from connection failure, it is recommended that both the remote and local NAS be on the same local network and that the remote NAS uses a static IP address. For other network related optimization settings (such as Port Trunking or Link Aggregation), please refer to the Network chapter.

Creating VJBODs with new iSCSI LUN (using Create Virtual JBOD's Disk Wizard)

> **Note:** Before you start this process, please ensure that the remote NAS has a storage pool with at least 154GB of free space.

Follow these steps to create a VJBOD:
1. Go to "Storage Manager" > "STORAGE" > "Disks/VJBOD".
2. Click "VJBOD" > "Create Virtual JBOD".
3. The Create Virtual JBOD's Disk Wizard will appear. Read the introductions and click "Next".
4. Establish a connection to a remote NAS:
   o Enter the remote NAS' IP address (or click "Detect" and select the NAS using its hostname or IP from the dropdown list). Or click "Local Host" to mount a LUN from the local host itself.
   o Enter the username and password used to log into the remote NAS (or the credentials of the local host if you select it in the last step).

- o Specify the system port and enable "Secure Connection (HTTP)" for a secure connection to the remote NAS.
  - o Use "Test" to test the connection settings.
  - o Click "Next".
5. Select "Create a new iSCSI LUN on the selected NAS".
   - o You can click "NAS Detail" in the top-right corner to check the storage status of the selected NAS.
   - o Tick "Host Binding" if the LUN will be used to store sensitive information.
   - o Click "Next".
6. Select a storage pool and click "Next".
7. Choose to set up CHAP authentication and enter the required information. Click "Next".
8. Set up the capacity for creating a new LUN and choose whether to enable 4K byte sector size and SSD cache in "Advanced Settings". Click "Next".
9. Review the configuration summary and click "Next".
10. Click "Finish" (you can also choose to [create a new storage pool](#), [new static volume](#), or recover existing data in this step).
11. The new VJBOD Disk will be created.

Note:
- The purpose of mounting a LUN from a local host itself is to ensure that the LUN will still be accessible if the original local host becomes unavailable.
- After ticking "Host Binding" in Step 5, the LUN can only be accessed by the bound host, even if the connection between the local host and remote NAS is lost (in this case, only the administrator of the remote NAS can access it).
- VJBOD currently only supports "Single" RAID configuration and cannot be used to create a system volume or expand other storage pools unless the pool also consists of VJBODs that come from the same remote NAS and same pool. The expanded capacity of the LUN on the remote NAS will not be reflected on the local host. Therefore, to expand a VJBOD pool, you can only create a new VJBOD on the same storage pool and join the disk into the pool as a new RAID.
- The LUN created here is a block-level iSCSI LUN.

Creating VJBODs with existing iSCSI LUN (using Create Virtual JBOD's Disk Wizard)

Note: Before you start this process, please ensure that the remote NAS has an idle target, storage pool with an instantly-allocated LUN and the capacity of the LUN is at least 154GB.

Follow these steps to create a VJBOD:
1. Go to "Storage Manager" > "STORAGE" > "Disks/VJBOD".
2. Click "VJBOD Beta" > "Create Virtual JBOD".

3. The Create Virtual JBOD's Disk Wizard will appear. Read the introduction and click "Next".
4. Establish a connection to a remote NAS:
   - Enter the remote NAS' IP address (or click "Detect" and select the NAS using its hostname or IP from the dropdown list). Or click "Local Host" to mount a LUN from the local host itself.
   - Enter the username and password used to log into the remote NAS (or the credentials of the local host if you select it in the last step).
   - Specify the system port and enable "Secure Connection (HTTP)" for a secure connection to the remote NAS.
   - Click "Test" to test the connection settings.
   - Click "Next".
5. Select "Choose an existing iSCSI LUN on the selected NAS". Click "Next".
6. Select a storage pool and click "Next".
7. Choose to set up CHAP authentication and select to use "Data Digest" and "Header Digest" (under "CRC/Checksum"). Click "Next".
8. Review the configuration summary and click "Next".
9. Click "Finish" (you can also choose to create a new storage pool, new static volume, or recover existing data in this step).
10. The new JBOD is created.

Using VJBODs

The VJBOD is essentially a space mapped from a LUN on a remote NAS. Before a VJBOD can be used to store data, a storage pool or volume must be created first. For volume or storage pool creation instructions, please check the relevant chapters (refer to the Volumes chapter for volume creation instructions and the Storage Pools chapter for storage pool creation instructions).

Managing and Monitoring VJBODs

Click a disk under "Virtual JBOD" in the system component panel to check its general information. Refer to the following table for actions available for managing a VJBOD:

Action	Description
Disk Info	Check details of the chosen VJBOD, including the remote NAS model, disk name, disk type, disk location, remote disk configuration, remote LUN name, remote iSCSI name, target IQN and disk capacity.
New Volume (under "Action")	Create a volume using the chosen VJBOD. Please refer to the chapter on Volumes for more information. Note that this action is only available for VJBODs without any volumes.
NAS Detail (under "Action")	Check details of the remote NAS where the LUN is located. The details include the hardware information, storage

	configuration, shared folders and installed applications.
Remote Log (under "Action")	Review logs (including information, warnings and errors) of the storage pool or NAS where the VJBOD disk is located. This will allow you to identify issues on the remote pool if the VJBOD becomes abnormal. You can click on the down arrow button on the "Log" page for advanced log search functionality.
Date Recovery (under "Action")	Recover the Volume or Storage Pool in VJBODs (if it exists). This action is only available when the VJBOD is idle.
Edit Disk (under "Action")	Edit the name of the chosen VJBOD.
Disconnect (under "Action")	Disconnect a VJBOD. Note that this action is only available for VJBODs that are in an abnormal status.
Connect (under "Action")	Reconnect a VJBOD. Note that this action is only available for VJBODs that are Disconnected.
Edit Target (under "Action")	Edit the VJBOD iSCSI connection and Remote NAS IP. Note that this action is only available for VJBODs that are Disconnected.
Delete (under "Action")	Delete a VJBOD connection configuration. Note that this action is only available for VJBODs that are Disconnected.

Alternatively, click on "Virtual JBOD" > "Virtual JBOD Overview" and check the following for each VJBOD disk:

- Disk details associated with the local host: The disk name, status, total size, storage pool and volume/LUN.
- Disk details associated with the remote host: The NAS name, storage pool, disk configuration, target & LUN name and CHAP.

VJBOD Virtual JBOD Overview

Initiator IQN: iqn.2004-04.com.qnap.ts-879.ripplevjbod ⓘ ↻   Safely Detach all

Disk Name	Status	Total Size	Host Storage Pool	Host Volume/LUN	Remote NAS	Remote Storage Pool	Remote Disk Configuration	Remote Target&LUN	CHAP
VJBOD 1	✓ Ready	1000.00 GB	⚠ Warning Storage Pool 3 1.45 TB	DataVol3,Data...	RippleTestNA... (192.168.0.10...	⚠ Warning Storage Pool 3 (114.42 GB Un...	RAID Group 3 Single 1 Disk(s)	Remote_VJBO...	Disabled
					iqn.2004-04.com.qnap.ts-879pro.iscsi.remote_vjbod1.c9df7a				
VJBOD 2	✓ Ready	500.00 GB	⚠ Warning Storage Pool 3 1.45 TB	DataVol3,Data...	RippleTestNA... (192.168.0.10...	⚠ Warning Storage Pool 3 (114.42 GB Un...	RAID Group 3 Single 1 Disk(s)	Remote_VJBO...	Disabled
					iqn.2004-04.com.qnap.ts-879pro.iscsi.remote_vjbod2.c9df7a				
VJBOD 3	✓ Ready	154.00 GB	--	--	RippleTestNA... (192.168.0.10...	⚠ Warning Storage Pool 3 (114.42 GB Un...	RAID Group 3 Single 1 Disk(s)	RemoteVJBO...	Disabled
					iqn.2004-04.com.qnap.ts-879pro.iscsi.remotevjbod1.c9df7a				

Note: Use this function or shutdown host NAS so the file system on those disks will not be affected during maintenance downtime. Detached file system can be recovered by selected "Scan All Free Disks" in "Disks/VJBOD" page.

> **Tip:**
> - If the firmware of the remote NAS is 4.2.2 (or newer), you can monitor what NAS has connected to an iSCSI LUN, as well as receive warnings if the iSCSI connection is lost on the "iSCSI Storage" page ("Storage Manager" > "iSCSI" > "iSCSI Storage").
> - If more detailed monitoring is required for multiple NAS, you can use Q'center to monitor both host and remote NAS.

Detaching and Reconnecting VJBODs

If a VJBOD has been used to create a virtual volume or storage pool, that volume or storage pool must be detached first before the VJBOD can be detached. Refer to the Volumes chapter for volume removal instructions and Storage Pools chapter for storage pool removal instructions. To detach a VJBOD disk, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Disks/VJBOD".
2. Select a VJBOD in the system component panel.
3. Click "Action" > "Disconnect".
4. Click "OK" and the VJBOD will enter "Disconnected" status.
5. Click "Action" > "Delete".
6. Check to remove the LUN and unused iSCSI target from the remote NAS and click "OK". The VJBOD will be deleted.

To reconnect disconnected VJBODs (there will be an error symbol in front of such disks), follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Disks/VJBOD".
2. Select a disconnected Virtual JBOD in the system component panel.
3. Click "Action" > "Connect".

4. Click "OK" and the VJBOD will enter the "Ready" status.

You can detach all of the VJBOD disks at once. To do so, go to the "Virtual JBOD Overview" page (click the "Virtual JBOD Overview" button in the top-right corner of the "Storage Manager" window) and click "Safely Detach all". Detached VJBODs can be re-attached by selecting "Recover" > "Scan All Free Disks" in the "Disks/VJBOD" page.

> **Note:** To protect the data and file system of VJBODs, always detach them before shutting down the remote NAS.

Data Roaming
You can move VJBODs from one NAS to another without needing to physically disconnect and reconnect drives. To do so, follow these steps:
1. Safely detach a VJBOD (refer to the Detaching and Reconnecting Virtual JBOD Disks section for instructions).
2. Open the Create Virtual JBOD's Disk Wizard on the NAS that you want to move the JBOD to and choose the existing iSCSI LUN on the remote NAS (refer to the Creating VJBOD with existing iSCSI LUN section for instructions).

Automatic Reconnection
The system will attempt to reconnect and recover a storage pool on a remote NAS for VJBODs after they become inaccessible for 30 seconds. However, the reconnection and recovery process may take longer if the remote NAS uses a dynamic IP (or it will fail if the two NAS are not on the same LAN). Therefore, we recommend using a static IP for the remote NAS.

> **Note:** If the remote NAS system port is changed, some information regarding the remote NAS may be incorrectly displayed on the host NAS. If this occurs, you can enter the updated information in the "Re-login" page (select the disk in "Disks/VJBOD" and click "Action" > "Re-login").
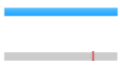
Storage Space

The Storage Space features Storage Pools and Volumes. This page lists available storage pools and the volumes, iSCSI LUNs, and snapshots from remote NAS on each of these storage pools. It displays these storage entities' capacity and/or usage to give a complete view of storage allocation. Users can create or manage storage pools/volumes/RAID groups, or take/view snapshots of the volumes on this page.
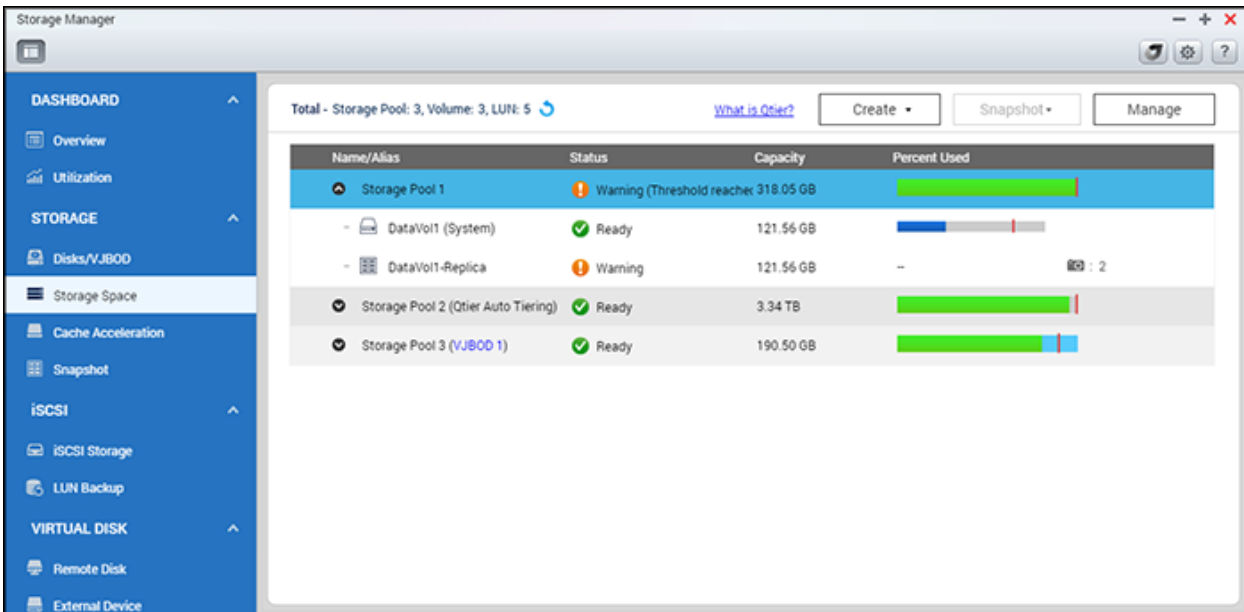
Below is a chart of what the icons and bars indicate.

Symbol	Name	Description
	Volume	Users may change the volume name. System volume names are appended with "(System)".
	LUN	Users may change the LUN name.
: 1	Snapshot	The number to the right of the camera icon indicates how many Snapshots are currently saved.
	Storage Pool Usage	Gray: Unallocated Green: Allocated Dark blue: Snapshot used Light blue: Snapshot reserved Red line: Alert threshold
	Volume Usage	Dark blue: Used Red line: Alert threshold

70

	LUN Usage	Light blue: Allocated
		Red line: Alert threshold

For details on Storage Pools, Volumes, and RAID Groups, refer to the following links:

- [Storage Pools](#)
- [Volumes](#)
- [RAID Groups](#)

Storage Pools

A storage pool is designed to aggregate physical hard disk drives into a large storage space and to provide enhanced RAID protection for it. You can perform the following actions to manage storage pools:

- Creating New Storage Pools
- Removing Storage Pools
- Safely Detaching Storage Pools
- Expanding Storage Pools
- Setting a Threshold
- Setting Snapshot Reservation
- Creating New Volumes for Storage Pools
- Creating New iSCSI LUNs for Storage Pools

Note:
- Storage Pools are not supported by some NAS models. Please refer to the QNAP website, product information, and software specifications for more details.
- For RAID groups that contain 16 hard drives, up to 512MB RAM will be used for them. 1GB RAM is recommended for 24-32 hard drives.

Creating New Storage Pools

Follow these steps to create a new storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Click "Create" > "New Storage Pool".
3. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk and click "Create".
4. Set the percentage of storage spool space that is reserved to store snapshots.
5. Please note that all data on the selected hard disk drive(s) will be erased. Click "OK" if you are certain about this.
6. A new storage pool will be created.

Removing Storage Pools

Follow these steps to remove a storage pool:
- Go to "Storage Manager" > "STORAGE" > "Storage Space".
- Double click a storage pool to be removed to bring up the Storage Pool Management page.
- Click "Remove" > "Remove Pool".
- Click "Apply".

- The selected storage pool will be removed.

> **Note:** Before you remove a storage pool, be sure to remove all volumes and LUNs on that storage pool.

Safely Detaching Storage Pools

Follow these steps to safely detach a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be removed to bring up the Storage Pool Management page.
3. Click "Remove" > "Safely Detach Pool".
4. Click "Apply".
5. The selected storage pool will be removed.

> **Note:** After a storage pool is reattached, the configurations of iSCSI LUNs mapped in the storage pool or Apps installed before the detachment will not be automatically recovered.

Expanding Storage Pools

Follow these steps to expand a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.
3. Click "Expand Pool".
4. Select to create and add a new RAID group. Select "Adding new hard drive(s) to an existing RAID group"(the option "Create new RAID groups" will be covered in the following section), choose an existing RAID group from the drop-down list and click "Next".
5. Select the hard drive(s) to expand the storage pool and click "Next".
6. Click "Expand".
7. Please note that all data on the selected hard disk drive(s) will be erased. Click "OK" if you are certain about this.
8. The chosen storage pool will be expanded.

> **Note:** New disks cannot be inserted into existing RAID groups of storage pools for specific RAID types (such as RAID 0, RAID 10, Single or JBOD). You must create an additional RAID group to expand those storage pools.

Expanding storage pools by creating new RAID groups

Follow these steps to create a RAID group for storage pool expansion:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.

3. Click "Expand Pool", select "Create and add a new RAID group" and click "Next".

4. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk and click "Next".

5. Please note that if the type of the newly-created RAID group is different from that of the existing RAID group(s), the performance of the entire storage pool may be affected. To continue, click "OK".

6. Click "Expand".

7. Please note that all data on the selected hard drive(s) will be erased. Click "OK" if you are certain about this.

8. The chosen storage pool will be expanded.

Note:

- RAID 0, JBOD or Single RAID Group cannot be added to a storage pool if that storage pool already contains RAID 1, 5, 6, or 10.
- It is recommended to set an independent storage pool on a JBOD and only add new disks to that JBOD (or replace the existing disks in that JBOD) when expanding the storage pool. Otherwise, data stored on that JBOD will become inaccessible when connecting that JBOD to a different NAS host.

Expanding storage pools by replacing hard disk drives in a RAID array

With this function, RAID group capacity can be expanded by replacing hard disk drives in an array one by one. This option is supported for the following RAID types: RAID 1, RAID 5, RAID 6 and RAID 10. Follow these steps to expand a RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.

3. Select a RAID group and click "Manage" > "Replace Disks One by One".

4. Select at least one hard disk drive and click "Change". After the description displays "Please remove this drive", remove the hard disk drive from the NAS or expansion enclosure.

5. After the description displays "You can replace this drive", plug in the new hard disk drive to the drive slot.

6. Repeat steps 4 and 5 until all hard drives have been replaced.

7. Click "Expand Capacity" to continue. Click "Yes".

8. The chosen RAID group is expanded.

Note: Available RAID management operations are detailed in the chapter on RAID Groups.

Setting a Threshold

The system will generate a warning message in system logs when the storage pool used size hits the threshold. To set a threshold value for a storage pool, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to set a threshold to bring up the Storage Pool Management page.
3. Click "Actions" > "Set Threshold".
4. Enter a value for alert threshold and click "Apply".

Setting Snapshot Reservation

You can set snapshot reservation space to ensure enough space for saving snapshots. Snapshot reservation is set as a percentage of total storage pool space and there are two scenarios:

- When the snapshot reserve is set to 0%, new snapshots taken will all be saved to a storage pool until that storage pool runs out of its space. When that happens, the system will start recycling older snapshots regardless the snapshot limitation set in Snapshot Global Settings.
- When the snapshot reserve is set to a value greater than 0%, this reserved space will be dedicated entirely to snapshots. The free space in a storage pool will be lower after the value is set and the snapshots will only use the space reserved. When the space used for snapshots exceeds the snapshot reserve, the system will start recycling older snapshots regardless the snapshot limitation set in Snapshot Global Settings.

To set snapshot reservation, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to set reserved space for snapshots and to bring up the Storage Pool Management page.
3. Click "Actions" > "Set Snapshot Reserved", enter a value for snapshot reserved space, and click "Apply".

> **Note:**
> - For more Snapshot details, refer to the Snapshot section in the Volumes chapter.
> - The function or its content is only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website.
>   - A minimum of 4 GB RAM is required to use snapshots.
>   - x51 series models only support up to 256 snapshots instead of 1024. The HS-251 does not support snapshots.

Creating New Volumes for Storage Pools

To create a new volume for a storage pool, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool.

3. Click "Create"> "New Volume". Follow the onscreen instructions to finish the creation process. For more details, please refer to the [Volumes](#) section.

Creating New iSCSI LUNs for Storage Pools

To create a new iSCSI LUN for a storage pool, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool.

3. Click "Create"> "New iSCSI LUN". Follow the onscreen instructions to finish the creation process. For more details, please refer to the [iSCSI Storage](#) section.

Volumes

A volume is formatted by the file system to store share folders and files. Users can manage, monitor, create, or delete a logical volume on this page. The following topics are covered in this chapter:

- [Creating New Volumes](#)
- [Removing Volumes](#)
- [Expanding Volumes](#)
- [Available Volume operations](#)
- [Configuring Alert Threshold](#)
- [Check File System](#)
- [Creating New Shared Folders](#)
- [Snapshot](#)
- [Managing Previous Versions in Windows](#)
- [Encryption](#)
- [Setting Thin Provisioning Space Reclamation and SSD Trim](#)

Creating New Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Click "Create" > "New Volume" to launch the volume creation wizard.
3. Configure the mode for the volume from static single, thick multiple, and thin multiple according to your needs (learn more about "Thick or Thin Volumes" in the following section) and click "Next".
4. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk for the volume to be created and click "Next".
5. Set the alert threshold and volume alias. You can also click "File system option" to specify bytes per inode, check the maximum volume size and number of files/folders, enable volume encryption, and create share folders. Click "Next".

Bytes per Inode	Max. Size of Volume	Max. Number of Files/Folders
4096	15.99 TB	Volume Size/Bytes per Inode
8192	31.99 TB	
16384 (Default	63.99 TB	

Bytes per Inode	Max. Size of Volume	Max. Number of Files/Folders
)		
32768	127.99 TB	
65536	250 TB	

6. Confirm your settings and click "Finish".
7. Please note that all data on the selected hard drive(s) will be erased. Click "OK" if you are certain about this.
8. The new volume will be created.

Note: The hot spare disk feature is only available for RAID 1, RAID 5, RAID 6 and RAID 10. For other RAID types, the hot spare disk field will be grayed out.

Follow these steps to create a new, thick or thin volume:
1. Select "Thick Multiple Volume" or "Thin Multiple Volume". Select to create a new storage pool or from an existing storage pool and click "Next".
2. Configure the mode for the volume from static single, thick multiple, and thin multiple according to your needs.
3. Configure the volume capacity, alert threshold, volume alias, Bytes per inode, encryption and shared folder settings and click "Next".
4. Click "Finish".
5. A new volume will be created.

Note:
- **Static Single Volume:** This mode offers the best performance but does not support thin provisioning, space reclamation and snapshots. For this option, the RAID group itself is a volume.
- **Thick Multiple Volumes:** This method can create multiple volumes on the same storage pool and instantly allocate physical storage space for the volume. It has better performance than thin volumes while also offering flexibility.
- **Thin Multiple Volumes:** Thin Multiple Volumes: This method can over-allocate the volume capacity for each volume regardless of the physical storage limit. Disk space is only used when files are written to the volume. After files are deleted, this space can be reclaimed for increasing the free space of the storage pool. The maximum size of thin multiple volumes is 20 times that of the storage pool's free space. With thin

Removing Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to be removed to bring up the Volume Management page.
3. Click "Remove". Click "Apply" and the selected volume is removed.

Expanding Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to be expanded to bring up the Volume Management page.
3. Click "Expand Volume".
4. Enter the desired capacity or click "Set to Max" to allocate the maximum available space for the volume and click "Apply". ("Set to Max" is only available for thick provisioned volumes.)
5. The capacity of the volume will be expanded.

Available Volume Operations

After you go to "Storage Manager" > "STORAGE" > "Storage Space", click "Actions" and choose to configure the threshold and cache settings, check the file system of a volume, rename volume alias, reclaim volume space, create a new share folder, format a volume, or manage snapshots.

Configuring Alert Threshold

The alert threshold is used to remind users when the capacity of a chosen volume is used up to the specified threshold level. A warning message will pop up when the specified threshold is reached. To set an alert threshold, select a volume in "Storage Space" to bring up the Volume Management page, click "Actions" > "Set Threshold", enter the threshold level and click "Apply". The alert threshold is set.

Check File System

If you receive the error message "File system is not clean", the NAS may have suffered an abnormal shutdown. The system data or files that were being used while the shutdown occurred may have been corrupted. To check the file system and repair possible errors, go to "Storage Manager" > "Storage Space".

Creating New Shared Folders

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to bring up the Volume Management page.
3. Click "Actions" > "Create New Shared Folder".
4. Specify the folder name and description of the new shared folder and select the disk volume for the shared folder.
5. Click "Edit" to the right of "Configure access privileges for users" in Step 4 and specify user privileges.
6. Click "Edit" to the right of "Advanced settings" in Step 4 and configure the guest access right, hidden folder, Oplocks, recycle bin and path. Click "Create".
7. A new shared folder will be created.

Snapshot

Users can take a snapshot, manage snapshots (revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files for LUNs or volumes), or replicate volumes/LUNs between different remote servers using snapshot technology.

> **Note:**
> - Snapshot Replica (or volumes/LUNs replication between remote servers) is covered in Backup Station. For details, please refer to the Snapshot Replica chapter in Backup

Taking a Snapshot

After reserved space is set, you can proceed to take snapshots. To create a snapshot, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a volume or LUN and click "Snapshot" > "Take a Snapshot".
3. Specify the snapshot name and duration to retain the snapshot.
4. Click "OK".

Managing Snapshots with Snapshot Manager

The Snapshot Manager allows you to take, revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files.

To launch Snapshot Manager, select a volume or LUN in "Storage Space" and click "Snapshot" > "Snapshot Manager" (or click the camera icon of a volume or LUN.)

In Snapshot Manager, you can perform the following actions:

- Restore files: Click a desired snapshot and select the folder(s) or file(s) that you want to restore, right click and select "Restore" to replace the existing folder/file with the one in the snapshot or "Restore to" to restore your data to a different location. Or choose "Download" to download the selection to your computer.

- Revert a snapshot: Select a snapshot and click "Revert", and the entire snapshot will be restored to its original path. Be cautious that the volume reverted to the selected snapshot will be in the previous state when the snapshot was taken.

- Delete: Select a snapshot and click "Delete" to delete that snapshot.

- Clone a snapshot: This action allows you to clone a snapshot into a new volume or LUN.   To clone a snapshot, first select a snapshot, click "Clone", enter an alias for the new volume, and select the folders to share after cloning. If the snapshot cloned is a LUN snapshot, you can map it to an iSCSI target.

- Set up snapshot schedules: Click "Schedule", select "Enable schedule", specify the time, frequency, and retention period. The system will take the chosen volume's snapshot by schedule. For Smart Snapshot, the system will only take a new snapshot if there are new changes made in the selected volume.

Snapshot Global Settings

Click "Global Settings" in the top-right of the Snapshot Manager window, and there is one global setting:

- Make snapshot directory (@Recently-Snapshot) visible: Mount a snapshot volume as a directory of a shared folder and set the snapshot volumes to be read-only in File Station. The snapshot directory will appear as "@Recently-Snapshot".

Click "Global Settings" in the top-right of the Storage Manager window, and there is one global setting:

- When reaching snapshot limitation: Choose the policy to handle snapshots when the snapshot limitation is reached. There are two choices.
  - Overwrite the oldest snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total) the oldest snapshot will be deleted in order to continue taking new snapshots for data protection.
  - Stop making snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total), no more new and scheduled snapshots will be taken until older snapshot are deleted. This option will prevent the deletion of older snapshots without administrators' consent.

> **Note:** The "When reaching snapshot limitation" setting uses the number of snapshots, not the space used for snapshots. For more details, please refer to the Setting Snapshot Reservation section.

Managing Previous Versions in Windows

Starting in QTS 4.2.1, snapshots can be used with the Previous Versions feature in Windows, allowing you to instantly revert to a previous version of a file in case of an accident (e.g. file deletion, corruption, or accidental changes.)

To use this feature, follow these steps:
1. In Windows, connect to a shared folder on the NAS (the shared folder must be located in a storage pool that you can take a snapshot.)
2. Take a snapshot of the storage pool where the shared folder is located.
3. In Windows, right click on the shared folder (or a file in that shared folder) in "File Explorer" > "Properties" > "Previous Versions".
4. Select a version and choose to open, copy, or restore that version.
5. Click "OK".

> **Note:** This feature is only applicable to files that have been changed between snapshots.

Encryption

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

Note: The AES volume-based encryption is applicable only to specific NAS models. Please refer to the [product comparison table](#) for details.

Data encryption on QNAP NAS

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

- Encryption password: Enter the encryption password to unlock the disk volume. The password must be 8-32 characters long. Symbols (! @ # $ % ^ & * ( )_+ = ? ") are supported.
- Encryption key file: Upload the encryption key file to the NAS to unlock the disk volume. The key can be downloaded from the "Encryption" page after the disk volume is successfully unlocked.

Before you start

Please remember the following before using the data encryption feature of the NAS.

- The volume encryption feature of the NAS is volume-based. A volume can be a single disk a JBOD configuration, or a RAID array. To only encrypt a shared folder, please refer to the [Shared Folder](#) chapter.
- Select whether or not to encrypt a disk volume before it is created on the NAS. A volume cannot be encrypted after it is created unless the disk volume is initialized. Note that initializing a disk volume will clear all data on the disks.
- Disk volume encryption cannot be removed without initialization. To remove encryption on the disk volume, the disk volume must be initialized and all the data will be cleared.
- Keep the encryption password or key safe. If the password is forgotten or the encryption key is lost, the data cannot be accessed and cannot be recovered.
- Before starting, read the instructions carefully and strictly adhere to them.

Note: Data encryption functions may be unavailable in accordance to the legislative restrictions of some countries (ex. Russia, Belarus, Ukraine, Kazakhstan and Uzbekistan.)

Creating new encrypted disk volumes

1. Log into the NAS as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space" and click "Create" > "New Volume".
2. Select a volume type based on your needs and click "Next".
3. Specify the volume details (including the volume capacity, alert threshold and volume alias,) tick "Encryption", fill out the encryption password and choose whether to save the encryption key, select to create a shared folder automatically after new volume initialization and fill out the name of the shared folder for the intended volume. Click "Next".
4. Confirm the settings and click "Finish".
5. Note that all the data on the selected drives will be DELETED! Please back up the data before creating the encrypted volume. Click "Yes" after data backup.
6. Double click the newly-created volume to bring up the Volume Management page.
7. Click "Actions" > "Encryption" > "Lock this Volume". Click "Yes".
8. An encrypted disk volume will be created on the NAS.

Encryption key management

To manage the encryption key settings, log into the NAS as an administrator and go to "Storage Manager" > "STORAGE" > "Storage Space". Double click a volume to bring up the Volume Management page and click "Actions" > "Encryption".

There are three options to manage the encryption key:

- Change the encryption key: Enter your old encryption password and the new password. (Please note that after the password is changed, any previously exported keys will not work anymore. The new encryption key needs to be downloaded if necessary, see below.)
- Download the encryption key file: Enter the encryption password to download the encryption key file. With this option, the encryption key can be saved as a file. The file is also encrypted and can be used to unlock a volume, without knowing the real password (see "Locking and unlocking disk volumes manually" below.) Please save the encryption key file in a secure place!
- Save the encryption key: Save the encryption key on the NAS to automatically unlock and mount the encrypted disk volume after the NAS restarts. **Note that saving the encryption key alone is not completely safe, as if the NAS is stolen, the volume will be automatically unlocked after it restarts.**

Locking and unlocking disk volumes manually

To lock a volume, log into the NAS as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". Double click a volume to be locked to bring up the Volume Management page and click "Actions" > "Encryption" > "Lock this Volume". Click "Yes".

To unlock a volume, log into the NAS as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". Select a volume to be unlocked and click "Manage" > " Unlock this volume". Choose either to enter the encryption password, or use the encryption key file exported previously. Click "Apply". If the encryption password or the key file is correct, the volume will be unlocked and become available.

Verifying encrypted disk volumes

To verify that a disk volume is encrypted, log into the NAS as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". The encrypted disk volume will be shown on this page, with a lock icon under "Status". The lock will be shown as opened if the encrypted volume is unlocked. A disk volume without the lock icon under "Status" is not encrypted.

Behaviors of encrypted volumes upon system reboot

An example is provided to illustrate the behavior of encrypted volumes upon system reboot. In this example, there are two encrypted disk volumes on the NAS:

- DataVol1 is created with the option "Save Encryption Key" disabled.
- DataVol2 is created with the option "Save Encryption Key" enabled.

Note: For details on enabling or disabling the "Save Encryption Key" option, please refer to the section on Encryption Key Management above.

After restarting the NAS, check the volume status. DataVol1 is locked, but DataVol2 is unlocked and mounted. Since the encryption key is not saved on DataVol1, the encryption password needs to be manually entered to unlock DataVol1. Please remember that by saving the key on the NAS, data will only be protected in case of stolen hard disk drives. However, there is still a risk of data breach if the entire NAS is stolen as the data is   accessible after the NAS is restarted. If the encryption key is not saved on the NAS, the NAS will be protected against data breach even if the entire NAS were stolen. The disadvantage is that the disk volume needs to be manually unlocked each time the system restarts.

Setting Thin Provisioning Space Reclamation and SSD Trim

Thin Provisioning Space Reclamation allows you to increase free space on thin-provisioned storage pools by reclaiming space from deleted files. SSD Trim enables garbage collection on SSDs, which wipes out blocks of data that are no longer in use, and increases future write performance.

To enable Space Reclamation and SSD Trim, log into QTS, launch Storage Manager and click on the "Global Settings" icon located at the top right of the Storage Manager window. The Global Settings window will open, then click on "Edit" beside Space Reclamation and SSD Trim. There are two settings for Space Reclamation and SSD Trim:

- **Auto reclaim and SSD trim schedule:** Check this checkbox to enable space reclamation and SSD trim.
- **Schedule:** Set the schedule for thin provisioning space reclamation and SSD TRIM in order to reclaim space and increase free space for storage pools.

RAID Groups

Users can expand a RAID group, add hard drive(s) to a RAID group, migrate a RAID group, configure a spare drive, enable a bitmap and recover a RAID group for a chosen volume, while the data contained in the RAID group remains intact. In this chapter, the following topics are covered:

RAID Group Introduction

RAID group types

Refer to the table below for explanations on RAID types:

Field	Description
Single Disk	A single, stand-alone RAID group can be set up for your NAS. However, this setup does not provide any redundancy protection. So, in the event that a disk is corrupted or otherwise damaged, all data on that disk will be lost.
RAID 0 Striping	A striping RAID group combines two or more disks into one large, logical disk. It offers the fastest disk access performance but no data redundancy protection in the event of disk failure or damage. The disk capacity is the sum of all disks. Disk striping is usually used to maximize disk capacity or to accelerate disk access speed. Please note that RAID 0 configuration is not recommended for storing sensitive data.
RAID 1 Mirroring	Disk Mirroring protects your data by automatically mirroring the contents of one disk to the second disk in the mirrored pair. It provides protection in the event of a single disk failure. The storage capacity is equal to the capacity of the smallest single disk, as the second disk drive is used to back up the first disk drive. RAID 1 configuration is suitable for storing sensitive data on a corporate or personal level.
RAID 5	RAID 5 configurations are ideal for organizations running databases and other

	transaction-based applications that require storage efficiency and data protection. A minimum of 3 hard disks are required to create a RAID 5 group. The total capacity of the RAID 5 group is equal to the size of the disk with the smallest capacity in the array times the number of (hard disk − 1). It is recommended (though not required) that only hard drives of the same brand and capacity are used to establish the most efficient hard drive capacity.
	In addition, if your system contains four disk drives, it is possible to use three drives to implement a RAID 5 data array with the fourth drive kept as a spare disk. In this configuration, the system will automatically use the spare disk to rebuild the array in the event of a physical disk failure. A RAID 5 configuration can survive one disk failure without losing any system functionality. When a disk fails in RAID 5, the disk volume will operate in the "degraded mode". There is no more data protection at this stage, and all the data will be lost if the unit suffers a second disk failure. A failed disk should be immediately replaced. Users can choose to install a new disk after turning off the server or hot-swap the new disk while the server is running. The status of the disk volume will change to "rebuilding" after installing a new disk. Your disk volume will return to a normal status once the volume rebuilding process is complete. **Note:** To install a new disk when the server is running, first ensure the disk volume is in "degraded" mode. Or, wait to hear two long beeps after the disk crashes and then insert the new disk in place of the failed disk.
RAID 6	RAID 6 is ideal for critical data protection needs. To create a RAID 6 group, a minimum of 4 hard disks are required. The total capacity of a RAID 6 group is equal to the size of the disk with the smallest capacity in the array times the number of (hard disks − 2). It is recommended (though not required) to use identical hard drives to establish the most efficient hard drive capacity. RAID 6 can survive 2 disk failures and the system can still operate properly. **Note:** To install a new disk when the server is running, first ensure the disk volume is in "degraded" mode. Or, wait to hear two long beeps after the disk crash and then insert the new disk in place of the failed disk.
RAID 10	RAID 10 is a combination of RAID 1 (mirroring) and RAID 0 (striping), without parity. RAID 10 is a stripe across a number of disks to provide fault tolerance and high speed data transfer. The storage capacity of a RAID 10 group is equal to the size of the disk with the smallest capacity in the array times (the number of hard disks in the array/2). It is recommended that only hard disk drives of the same

	brand and capacity are used to create a RAID 10 group. RAID 10 is suitable for high volume transaction applications, such as a database, that require high performance and fault tolerance. A maximum of 1 failed disk from each disk pair is allowed in RAID 10. **Note:** To install a new disk when the server is running, first be sure the disk volume is in the "degraded" mode. Or, wait to hear two long beeps after the disk crashes and then insert the new disk in place of the failed disk.
JBOD	Two or more disks can be combined into one larger volume. Files are sequentially saved on physical disks. The overall capacity of the linear disk is the sum of the capacity of all disks. This configuration does not provide disk failure protection; failure of one drive will cause the entire array to be lost. A JBOD group is generally used for storing a large amount of data. It is not appropriate for storing sensitive data.

Bad Block Management (BBM)

BBM uses the bad block list (log) for each drive and uses it to allow the system to fail single blocks rather than entire drives. This feature is especially useful for RAID arrays and is automatically enabled if your disks support BBM. Bad blocks in different sections on different drives can cause a RAID array to fail. With BBM, the RAID array can be functional even when encountering bad blocks.

Note: BBM support is only available for RAID 5 and RAID 6.

Expanding RAID Group Capacity

With this function, RAID group capacity can be expanded by replacing hard disk drives in a RAID group array one by one. This option is supported for the following RAID types: RAID 1, RAID 5, RAID 6 and RAID 10. Follow these steps to expand a RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Replace Disks One by One".
4. Select at least one hard disk drive. After the description displays "Please remove this drive", remove the hard disk drive from the NAS or expansion enclosure.
5. After the description displays "You can replace this drive", plug in the new hard disk drive to the drive slot. Repeat the same process for all hard drives to be replaced. Click "Expand Capacity" to continue.
6. Click "Yes".
7. The chosen RAID group is expanded.

Adding Hard Disk Drives

With this function, new drive members can be added to a RAID group. This option is supported for RAID 5 and RAID 6 drive configurations.

Follow these steps to add the hard disk drive(s) to a RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Add Hard Drive".
4. Select hard disk drive(s) from the list to add to the chosen RAID group and click "Apply".
5. Please note that all data on the selected hard drive(s) will be erased. Click "Yes" if you are certain about this.
6. The chosen hard disk drive(s) are added to the selected RAID group.

> **Note:** New disks cannot be inserted into existing RAID groups for specific RAID types, such as, RAID 0, RAID 10, Single, or JBOD. You must create additional RAID groups to expand these storage pools.

Migrating RAID Configuration

With this function, a RAID configuration can be migrated to a different RAID configuration. This option is supported for the following drive configurations: Migrating single drives to RAID 1; Migrating RAID 1 to RAID 5; Migrating RAID 5 to RAID 6. Follow these steps to migrate a RAID configuration:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Migrate".
4. Select the hard disk drive(s) from the list and click "Apply".
5. Please note that all data on the selected hard disk drive(s) will be erased. Click "Yes" if you are certain about this.
6. The chosen RAID configuration is migrated to the new one.

Configuring Spare Drives
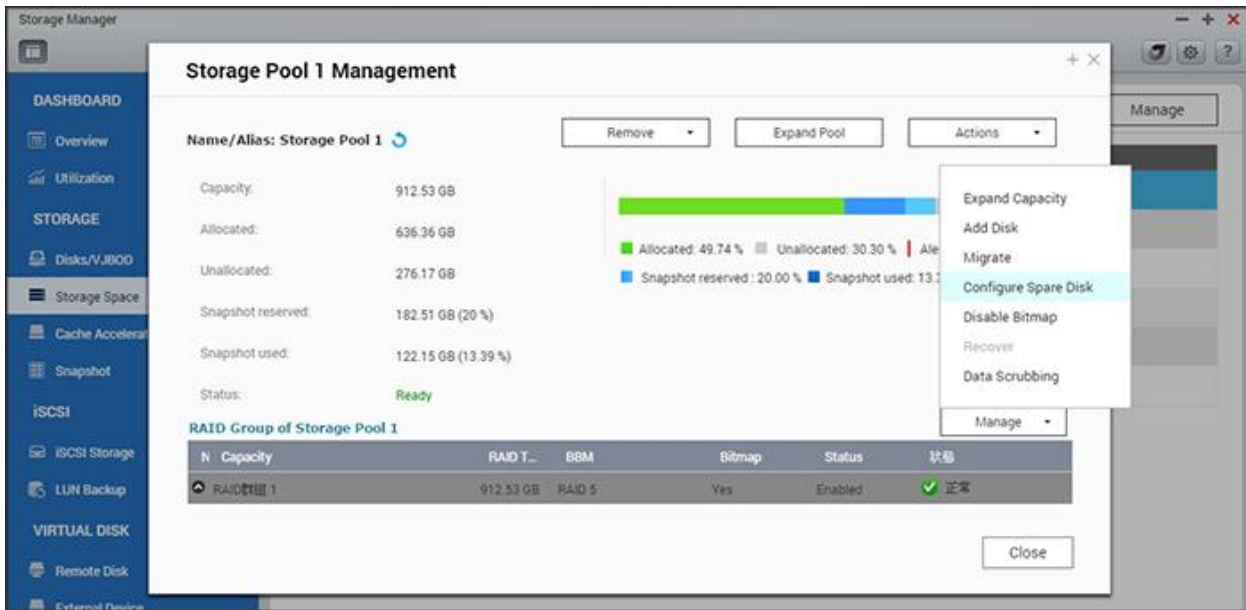
With this function, a spare drive can be added to or removed from a RAID 1, RAID, 5, RAID 6, or RAID 10 configuration. Unlike a global spare drive, the drive in this case will be dedicated to the RAID group. Follow these steps to configure a spare drive:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Configure Spare Drive".
4. Select the hard disk drive(s) to be configured as spare drive and click "Apply".
5. Please note that all data on the selected hard disk drive(s) will be erased. Click "Yes" if you are certain about this.
6. The chosen disk drives are added as spare drive.

Enabling/Disabling Bitmap

This function can reduce the rebuild time after a crash, or the time length required to remove/re-add a hard disk. This feature does not improve disk read/write performance and may even cause slight performance degradation. However, if an array has a bitmap, a hard disk can be removed and re-added, and only changes in blocks need to be made since the removal (as recorded in the bitmap) can be re-synced. To enable a bitmap, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Enable Bitmap" and then "OK".

To disable a bitmap,

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool to bring up the Storage Pool Management page.

3. Select a RAID group and click "Manage" > "Disable Bitmap" (only available after a bitmap has been enabled) and then "OK".

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

Recovering Failed RAID Disk Volumes

This can recover failed RAID disk volumes from the "Inactive" status to a normal state (RAID 1, RAID 5, RAID 6 and RAID 10 will be recovered to the degraded mode; RAID 0 and JBOD will be recovered to the normal state.) Before recovering a failed disk volume, please confirm that all hard disks of that disk volume are properly seated in the NAS drive bays. Once recovery is completed, immediately back up your data on the disk(s) in case the disk volume fails again.

Inactive RAID disk volumes can only be recovered if the minimal number of healthy disks required for the RAID configuration is available on the NAS. For example, in a RAID 5 configuration with three disks in the array, at least two healthy hard disk drives are required available in the NAS for volume recovery. If not, this RAID volume cannot be recovered. Refer to the following table for the minimal number of hard disks required to recover a RAID group:

RAID group	Minimal number of hard disks required for recovery
RAID 1	1
RAID 5	Number of disks - 1
RAID 6	Number of disks - 2
RAID 10	Number of disks / 2; (1 hard drive per RAID 1)

Follow these steps to recover a failed RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".

2. Double click a storage pool to bring up the Storage Pool Management page.

3. Select a failed RAID group.

4. Click "Manage" > "Recover".

5. The chosen RAID group will be recovered.

Data Scrubbing

Data Scrubbing scans the sectors of RAID groups and automatically attempts to repair failed sectors to maintain the consistency of the file system. This function is only supported by   RAID 5 and RAID 6 and cannot be performed on a RAID Group that is in degraded mode. We recommend setting up a scheduled task for this function to avoid losing any critical data in the event of disk failure. Note that read/write performance may be affected during data scrubbing.

Cache Acceleration

Based on SSD technology, the Cache Acceleration feature is designed to boost access performance of the NAS. On this page, you can both monitor SSD performance and manage cache acceleration for your NAS. This chapter covers the following topics:

- Feature Requirements
- Creating SSD Volumes
- Removing SSD Volumes
- Expanding SSD Volumes
- Configuring Volumes for SSD Cache

Feature Requirements

SSD drives must be installed to enable this function and this feature is only available for certain NAS models, with memory requirements. Refer to the following link for details:

https://www.qnap.com/i/en/enterprise_apply_v2/con_show.php?op=showone&cid=7

Refer to the table below for memory requirements:

Cache Capacity	RAM Requirement*
512 GB	from 1 GB to 4 GB
1 TB	from 4 GB to 8 GB
2 TB	from 8 GB to 16 GB
4 TB	Above 16 GB

*For example, for 1 TB of SSD capacity, at least 4GB RAMs are required for the NAS.

On this page, users can choose to create, remove and expand a SSD volume and configure the SSD cache.

Note: You can toggle this feature by clicking the switch button right above "Usage".

Creating SSD Volumes

Follow the steps below to create a SSD volume:

1. Click "Create".
2. Select the SSD drive(s) and cache algorithm to create a SSD cache volume.
3. Select the cache type: Read-Only or Read/Write. Click "Next".

4. Choose the SSD Cache Mode:
   - Accelerate random I/O: Only small random I/O will be stored in SSD cache. This mode is recommended for virtualization and database applications. Also, select the bypass block size under this mode (block sizes that are larger than the specified one will not be cached).
   - Accelerate sequential I/O: All I/O will be stored in SSD cache. This mode is recommended for video streaming or large file access operations.
5. Select (or deselect) from the list to enable (or disable) the SSD cache for each iSCSI LUN and Volume.
6. Click "Create".
7. Please note that all of the data on the selected hard drive(s) will be erased. Click "OK" to confirm.
8. An SSD cache volume will be created.

Note: If SSD Cache is enabled with the Read-Write type, the SSD MUST NOT be removed while it is being used, as this will cause data loss.

Removing SSD Volumes

Follow the steps below to remove a SSD volume:
1. Click "Remove".
2. Please note that all data on the selected hard drive(s) will be erased. Click "Yes" if you are certain about this.
3. The SSD volume will be removed. This operation can take a prolonged period if the SSD Cache is in Read/Write mode, as all the data in the cache must be flushed to the hard drive first.

Expanding SSD Volumes

Follow the steps below to expand a SSD volume:
1. Click "Add SSD Drive".
2. Select the SSD drive(s) from the list and click "Expand".
3. Please note that all data on the selected hard drive(s) will be erased. Click "Yes" if you are certain about this.
4. The SSD volume will be expanded.

Configuring Volumes for SSD Cache

Follow the steps below to configure volumes for a SSD cache:
1. Click "Cache Setting".
2. Select or deselect a volume to enable/disable the SSD cache, choose whether or not to record large block, sequential I/O operations in the cache space, and click "Finish".

3. The settings will be applied to the chosen volume.

> **Note:**
> - For larger block, sequential I/O operations such as video streaming, the hit rate is lower, and by default, they are not recorded in the cache space. If you need to record such operations, please cancel this setting, but please remember that after this setting is cancelled, more cache space and computing resources will be consumed for such operations.
> - Not all applications can benefit from a SSD cache. Please make sure that the SSD cache is supported by your applications.

Snapshot

Snapshot Vault stores snapshots created remotely from remote NAS via Snapshot Replica in Backup Station. It also lets you manage and restore remote snapshots.
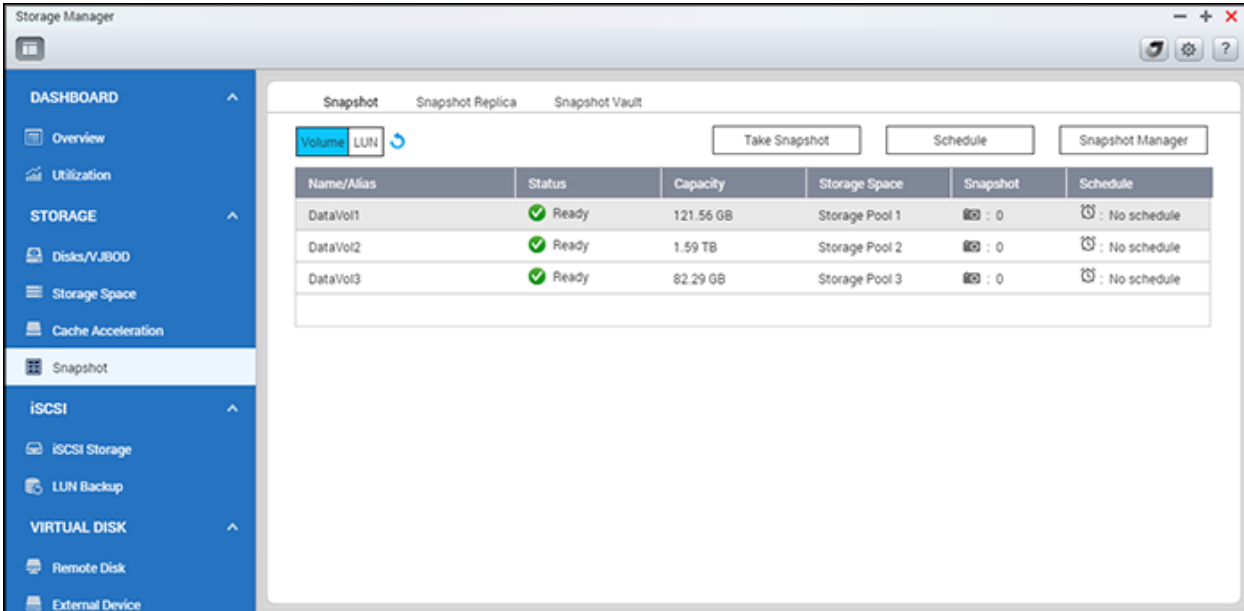
In this chapter, the following topics are covered:

- Snapshot
  - Taking a Snapshot
  - Managing Snapshots with Snapshot Manager
  - Snapshot Global Settings
  - Managing Previous Versions in Windows
- Snapshot Vault
  - Filtering Snapshots
  - Displaying Snapshot Content
  - Removing Snapshots
  - Cloning Snapshots

> **Note:**
> - Snapshot Replica (or volumes/LUNs replication between remote servers) is covered in Backup Station. For more details, please refer to the Snapshot Replica chapter in Backup Station.
> - Snapshots and related features are currently only available for the following NAS series: x51*, x53, x63, x70, x71, x79, x80, x82, x89.
>   - * The NAS must have minimum of 4 GB RAM to use snapshots.

Snapshot

Taking a Snapshot

After a reserved space is set, you can proceed to take snapshots. To create a snapshot, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Snapshot".
2. Switch between "Volume" or "LUN" depending on your needs, select a volume/LUN, and click "Take a Snapshot".
3. Specify the snapshot name, duration to retain the snapshot and snapshot type (the snapshot type is only available for LUN snapshots).
4. Click "OK".

Managing Snapshots with Snapshot Manager

To open Snapshot Manager, select a volume or LUN in "Storage Space" and click "Snapshot" > "Snapshot Manager". Alternately, you can click the camera icon of a volume or LUN.

Snapshot Manager enables you to perform the following actions:

Action	Description

View snapshot details	Select one of the following views:
	• Table view: Displays a chronological list of all snapshots
	• Timeline view: Displays a timeline containing all snapshots created within a specific period and other information, including the following:
	  o Snapshot details: Name, date and time of creation, status, file size, and description
	  o Volume details: Shared folders and files

Restore and download files	1. Click a snapshot and select the folders and files that you want to restore.
	2. Right-click one of the following:
	  o "Restore": Replaces the existing folder/file with the one in the snapshot
	  o "Restore to": Restores data to a different location
	  o "Download": Downloads the selection to your computer

Revert snapshots	Select a snapshot and click "Revert" to restore the snapshot to its original path.
	Warning: The volume reverted to the selected snapshot will the snapshot was taken.
Clone snapshots to new volumes or LUNs	1. Select a snapshot and click "Clone". 2. Type an alias for the new volume, and select the folders to share after cloning.
	Note: You can map cloned LUN snapshots to iSCSI targets.
Delete snapshots	Select a snapshot and click "Delete" to delete that snapshot.
Configure snapshot schedules	1. Click "Schedule". 2. Select "Enable schedule" and specify the time, frequency, and retention period.
	Note: For Smart Snapshot, the system takes a new snapshot made in the selected volume.

Snapshot Global Settings

There are two global snapshot settings:

In the Snapshot Manager window: Click "Snapshot global settings" (the gear icon) in the top-right corner of the Snapshot Manager window. There is one global setting:

- Make snapshot directory (@Recently-Snapshot) visible: Mount a snapshot volume as a directory of a shared folder and set the snapshot volumes to be accessed (read-only) in File Station. The snapshot directory will appear as "@Recently-Snapshot".

In the Storage Manager window: Click "Global Settings" (the gear icon) in the top-right corner of the Storage Manager window, and there is one global setting:

- When reaching snapshot limitation: Choose the policy to handle snapshots when the snapshot limitation is reached. There are two choices.
  - Overwrite the oldest snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total) the oldest snapshot will be deleted in order to make space for new snapshots.
  - Stop making snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total), no more new and scheduled snapshots will be taken until existing snapshots are deleted. This option will prevent the deletion of older snapshots without administrators' consent.

Note: The "When reaching snapshot limitation" setting uses the number of snapshots, not the space used for snapshots. For more details, please refer to the Setting Snapshot

Managing Previous Versions in Windows

Starting with QTS 4.2.1, snapshots can be used with the Previous Versions feature in Windows, allowing you to instantly revert to a previous version of a file in the event of an accident (e.g. file deletion, corruption, or accidental changes.)

To use this feature, follow these steps:

1. In Windows, connect to a shared folder on the NAS (the shared folder must be located in a storage pool where snapshots can be taken.)
2. Take a snapshot of the storage pool where the shared folder is located.
3. In Windows, right click on a shared folder (or a file in that shared folder) in "File Explorer" > "Properties" > "Previous Versions".
4. Select a version and choose to open, copy, or restore that version.
5. Click "OK".

Note: This feature is only applicable to files that have been changed between snapshots. Otherwise, there will be no previous versions listed in "File Explorer" > "Properties" > "Previous Versions".

Snapshot Vault

Snapshot Vault stores snapshots that are created by remote NAS devices and sent through Snapshot Replica in Backup Station. Snapshot Vault also allows you manage and restore remote snapshots, and replicate entire vaults to remote NAS devices.

Note:
- If this is the first time using this feature, please configure Snapshot Replica in Backup Station on the source NAS first.
- Snapshots and related features are currently only available for the following NAS series: x51*, x53, x63, x70, x71, x79, x80, x82, x89.
  - * The NAS must have minimum of 4 GB RAM to use snapshots.
  - * x51 series models only support up to 256 snapshots instead of 1024. The HS-251 does not support snapshots.

Snapshot Vault enables you to perform the following actions:

Action	Description
Filter snapshots	Go to "Storage Manager" > "Snapshot" > "Snapshot Vault" to see a list of available snapshots. You can filter snapshots using the following criteria: • Source: Source NAS IP address • Volume/LUN: Replicated volume or LUN • Location: Storage pool that contains the snapshot • Status: Snapshot status **Note:** If the status of a snapshot is not "Ready", you will not that snapshot.
Display content	1. Go "Storage Manager" > "STORAGE" > "Snapshot" > "Snapshot Vault". 2. Select a snapshot from the list and click "Show Snapshots". The screen displays the following information: • Left panel: Overview of snapshots • Right panel: Folders and files in the snapshots **Note:** To review advanced information in an expanded windo content" next to the search box.
Download content	1. Go "Storage Manager" > "STORAGE" > "Snapshot" > "Snapshot Vault". 2. Select a snapshot from the list and click "Show Snapshots". 3. Click "Show snapshot content". 4. Select the files that you want to download, right-click, and then select "Download".
Remove snapshots	1. Go to "Storage Manager" > "STORAGE" > "Snapshot" > "Snapshot Vault". 2. Select a snapshot in the list and click "Remove".

Filtering Snapshots

Navigate to Snapshot Vault in "Storage Manager" > "Snapshot" > "Snapshot Vault" and you will see a list of available snapshots. You can click the filter drop down list to filter snapshots with a set of criteria:

• Source: Source NAS IP address
• Volume/LUN: The volume/LUN that has been replicated
• Location: The storage pool where the snapshot has been stored
• Status: The snapshot status

> **Note:** If the status of a snapshot is not "Ready", you will not be able to view or access that snapshot.

Displaying Snapshot Content

Navigate to Snapshot Vault in "Storage Manager" > "STORAGE" > "Snapshot", choose the desired snapshot replication from the list, and click "Show Snapshots" to display its content. You can see an overview of snapshots in the left panel or browse through folders and see files in the snapshots on the right panel.

Click the "Hide snapshot content" button next to the search box to review advanced information regarding snapshots in an expanded window.

To download files in a snapshot, click the "Show snapshot content" button, select the files, right click your mouse and click "Download".

Removing Snapshots

1. Navigate to Snapshot Vault in "Storage Manager" > "STORAGE" > "Snapshot".
2. Select a snapshot replication in the list and click "Remove".
3. The snapshot replication is removed.

Cloning Snapshots

1. Navigate to Snapshot Vault in "Storage Manager" > "STORAGE" > "Snapshot".
2. Select a snapshot replication in the list and click "Show Snapshots".
3. Select a snapshot on the left panel and click "Clone".
4. Enter a name for the volume to mount the snapshot.
5. Choose the folders/files to clone.
6. Select "OK" and the task will start immediately.
7. Go to "Storage Manager" > "STORAGE" > "Storage Space" and you will see the new volume that has been cloned from Snapshot Vault.
8. You can now also use File Station to manage the files in the new volume.

Qtier

Qtier is an automated-tiering storage solutions that moves hot data to high-performance storage tiers and cold data to lower-cost, higher-capacity drives, allowing users to enjoy exceptional application performance and lower TCO of storage at the same time. This chapter covers the following topics:

- Creating Storage Space with Qtier
- Managing Auto Tiering
- Monitoring Auto-Tiering Performance

> **Note:** This function or its content is only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website.

Creating Storage Space with Qtier

1. Install at least two different types of drives (SSD, SAS, or NL-SAS) in the NAS. One of the types of drives must be SSDs.
2. Create a new storage pool in "Storage Manager" > "Storage Space" > "Create" > "New Storage Pool" or "Storage Manager" > "Storage Space" > or "Storage Manager" > "Storage Space" > "New Storage Pool".
3. The storage pool creation wizard will appear, check "Enable Qtier" and click "Next".
4. Select the SSD drives to be used to build the ultra-high speed tier in the storage pool. Select RAID type and Hot Spare Disk. Click "Next".
5. Configure the Snapshot settings in the "Snapshot Protection Settings" section, then click "Create". A confirmation box will appear informing you that the data on the selected disks will be erased if you continue. To continue, click "OK".
6. The "Expandable Qtier Tiered Storage Pool" window will appear, click "OK" to create other tiers. At least two tiers must be created.
7. Proceed to create different tiers. Select the drives to build other tiers. Select RAID type and Hot Spare Disk. Review summary and click "Expand" to continue. A confirmation box will appear informing you that the data on the selected disks will be erased if you continue. To continue, click "OK".
8. The "Expandable Qtier Tiered Storage Pool" window will appear.
   - To continue expanding the Qtier tiered storage pool, click "OK". Select the drives to expand the storage pool. Select RAID type and Hot Spare Disk. Review summary and click "Expand" to continue.
   - If you are done expanding this storage pool, click "Cancel".

9. The "Qtier Auto Tiering Schedule Settings" window will appear. Choose to reallocate data automatically during system idle time or during a specified schedule. Select "Apply".

> **Note:**
> - As relocation may affect the storage I/O performance, it is recommended to schedule this action during off-peak hours or when the storage is not frequently used.
> - Auto Tiering cannot be started immediately after a storage pool is created, as it will need time to retrieve information on when data is accessed. It also cannot be scheduled for full time, otherwise the data access pattern may not be accurate.

Managing Auto Tiering

Go to "Storage Manager" > "Storage Space" and double click on a Qtier Auto Tiering Storage Pool to bring up the "Storage Pool Management" window. Select "Qtier Auto Tiering". The following actions are available:

Action	Description
Relocation Schedule	- Automatically reallocate data when the system is idle. - The system will attempt to reduce the performance impact by only reallocating data to different tiers when the system is idle. - Enable Qtier Auto Tiering Schedule. - The administrator can manually set the data relocation schedule to low load times to reduce performance impact.
Statistics	Review the general information for each tier and history report.
Manage > Stop Relocations	Stop allocation.
Manage > Set Allocation Level	Set the default data allocation tier and data reservation ratio for ultra-high speed tier. - Default data allocation tier: Set which tier new data will be stored in. - Data reservation ratio for the ultra-high speed tier: Choose the amount of data to retain in the ultra high-speed tier (even though they are cold data.)

Monitoring Auto-Tiering Performance

On the Storage Pool Management dialog (bottom of the dialog), the current auto-tiering settings and performance will be listed:

- Relocation status: Indicates if auto-tiering is active (or idle).
- Enable schedule: Indicates if the schedule is enabled.
- Data reservation ratio for ultra-high speed tier: Indicates the amount of data currently set to be retained in the ultra-high speed tier.
- Amount of data optimized for performance: Shows the amount of data that has been allocated to high-speed tiers (or the "Move Down" or "Move Up" columns in "Manage" > "Statistics") in the last auto tiering schedule.
- Amount of data optimized for capacity: Shows the amount of data that have been allocated to high speed tiers (or the "Move Down" or "Move Up" columns in "Manage" > "Statistics") in the last auto tiering schedule.
- Data allocation priority: Indicates whether data will be written on the SSD tier if the "ultra-high speed" is set in "Manage" or first written on the SATA tier and then the SSD if "Capacity" is set in "Manage"

Additionally, you can check the history report ("Manage" > "Qtier Auto Tiering" > "Statistics") for further details on auto-tiering performance, including data moved up/down in a task, total used space after task completion and the current tasks with a trend chart.

iSCSI

Manage the iSCSI storage, create advanced ACLs and back up LUNs with the iSCSI management features.
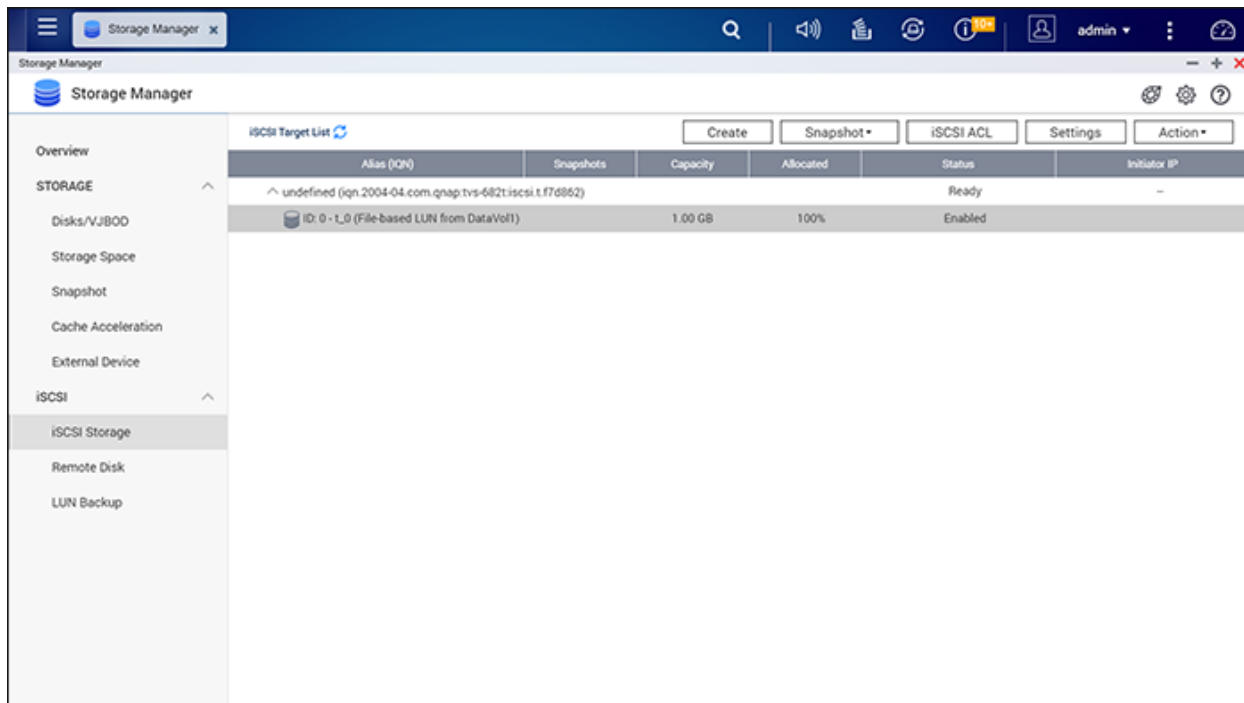
For details on the features, please refer to the following links:

* iSCSI Storage
* LUN Backup

iSCSI Storage

The NAS supports a built-in Internet Small Computer System Interface (iSCSI) service for clustered and virtualized environments.
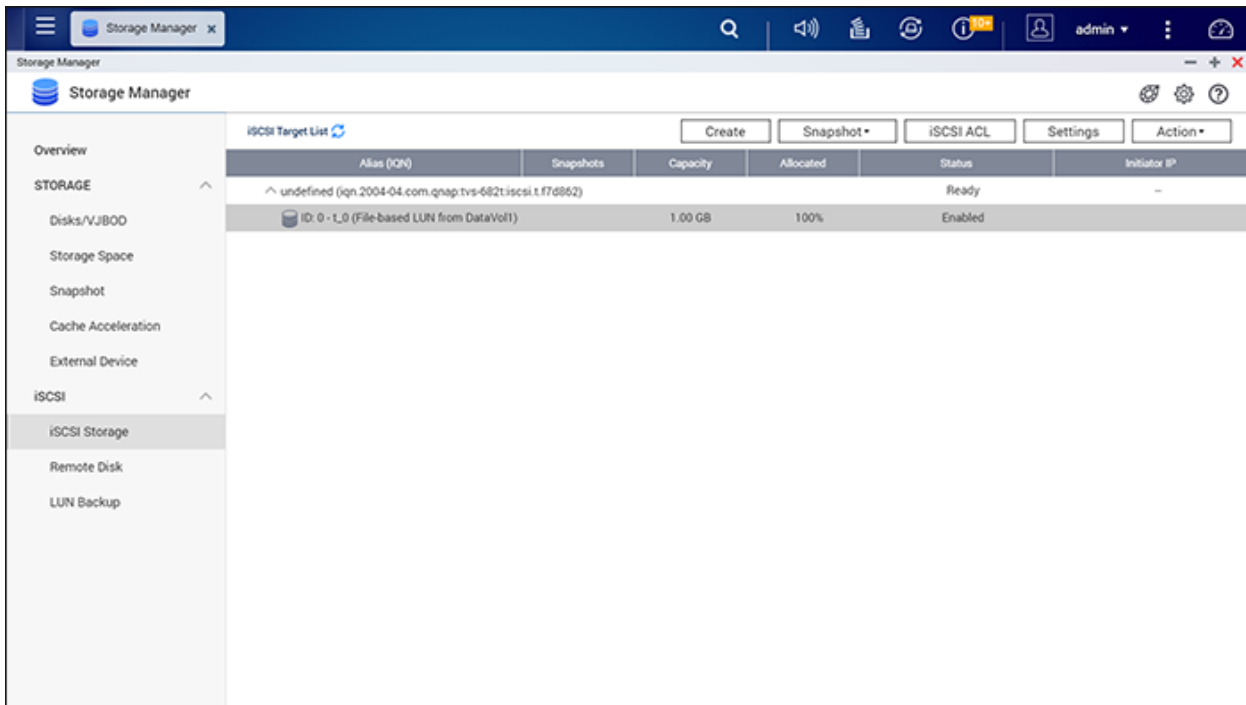
An iSCSI storage network includes the following nodes:
- Target: Storage device that contains one or more LUNs, which are logical units of storage
- Initiator: Client that initiates connections (through SCSI commands) to the storage device, which is called a target

> **Note:** In the context of your network, your computer (an initiator) connects to the NAS and retrieves the following:
> - List of available targets
> - List of available LUNs in each target

In addition to enabling and disabling the service, users can perform the following tasks:
- Configure the port of the iSCSI portal
- Enable or disable the Internet Storage Name Service (iSNS) service
- Manage all iSCSI targets and LUNs, including mapping and unmapping of LUNs to specific targets

> **Note:** The NAS supports multiple iSCSI targets and multiple LUNs per target.

In this chapter, these topics are covered:

- [iSCSI Configuration](#)
- [Optimizing iSCSI Performance](#)
- [Advanced ACL](#)
- [Snapshot](#)

Note: The function or its content is only applicable on some models. To check for applicable models, please refer to the [product comparison table](#) on the QNAP website.

iSCSI Configuration

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

1. Install an iSCSI initiator on the computer (Windows PC, Mac, or Linux).
2. Create an iSCSI target on the NAS.
3. Run the iSCSI initiator and connect to the iSCSI target on the NAS.
4. After successful logon, format the iSCSI target (disk volume). The disk volume on the NAS can then be used as a virtual drive for the computer.

Between the computer and the storage device, the computer is called an initiator because it initiates the connection to the device, and the storage device is referred to as a target. An iSCSI LUN is a logical volume mapped to the iSCSI target and there are two types of LUNs: file-based LUN and block-based LUN. File-based LUN is the legacy LUN, while block-based LUN is available for certain NAS models. Please refer to the [product comparison table](#) for details.

The table below lists the features supported by block-based LUNs and file-based LUNs:

	Block-based LUN (recommended)	File-based LUN (Legacy)
VAAI Full Copy	Supported	Supported
VAAI Block Zeroing	Supported	Supported
VAAI Hardware Assisted Locking	Supported	Supported
VAAI Thin Provisioning and Space Reclaim	Supported	Not Supported
Thin Provisioning	Supported	Supported
Space Reclamation	Supported (With VAAI or from Windows Server 2012,	Not Supported

	Windows 8 or later versions)	
Microsoft ODX	Supported	Not Supported
LUN Backup	Supported	Supported
LUN Snapshot	Supported	1 Time Snapshot (With LUN Backup)

Please note that in general, better system performance can be achieved through block-based LUNs, thus it is recommended to use block-based LUNs whenever possible.

There are two methods a LUN can be allocated: Thin Provisioning and Instant Allocation:

- Thin Provisioning: Allocate the disk space in a flexible manner. The disk space can be allocated to the target anytime regardless of the current storage capacity available on the NAS. Over-allocation is allowed as the storage capacity of the NAS can be expanded using online RAID capacity expansion.
- Instant Allocation: Allocate the disk space to the LUN instantly. This option guarantees the disk space assigned to the LUN but may require more time to create the LUN.

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 network infrastructure and application performance. Excessive concurrent connections may impact NAS performance.

> **Note:**
> - It is NOT recommended to connect to the same iSCSI target with two different clients (iSCSI initiators) at the same time, as it may lead to data loss or disk damage.
> - For ARM-based NAS models, the maximum volume capacity supported for online RAID capacity expansion is 8TB.

iSCSI Quick Configuration Wizard

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

1. If no iSCSI targets have been created yet, the Quick Configuration Wizard will automatically be launched and prompt users to create iSCSI targets and LUNs.
2. Select "iSCSI Target with a mapped LUN" (more on "iSCSI target only" and "iSCSI LUN only" in the following sections) and click "Next".
3. Click "Next."
4. Enter the target name and alias.

5. Only use "Enable clustering access to the iSCSI target from multiple initiators" for cluster-aware file systems such as VMware Virtual Machine File System. The "Data Digest" and "Header Digest" are optional fields (expand on "CRC/Checksum") and are the parameters for which the iSCSI initiator is verified when it attempts to connect to the iSCSI target. Click "Next."

6. Enter the CHAP authentication settings and click "Next". Check "Use CHAP authentication" and only the initiator will be authenticated by the iSCSI target, and users of the initiators are required to enter the username and password specified here to access the target. Check "Mutual CHAP" for two-way authentication between the iSCSI target and the initiator. The target authenticates the initiator using the first set of username and password. The initiator authenticates the target using the "Mutual CHAP" settings. For username and password limitation on both fields, refer to the following:

   o Use CHAP authentication:
     - **Username limitation:** The only valid characters are 0-9, a-z, A-Z and the maximum length is 128 characters.
     - **Password limitation:** The only valid characters are 0-9, a-z, A-Z and the maximum length: 12-16 characters

   o Mutual CHAP:
     - **Username limitation:** The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) and the maximum length: 12-16 characters
     - **Password limitation:** The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) and the maximum length: 12-16 characters

7. Choose the LUN type and LUN allocation method, enter the name of the LUN and specify the LUN location (disk volume on the NAS), the capacity and alert threshold for the LUN. Click "Next".

8. Confirm the settings and click "Next".

9. Click "Finish".

10.   The target and LUN will both show up on the list.

Creating iSCSI targets

Follow the steps below to create an iSCSI target:

1. Click "Create".

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

3. Only use "Enable clustering access to the iSCSI target from multiple initiators" for cluster-aware file systems such as VMware Virtual Machine File System.

4. Enter the target name and alias. Choose to click "CRC/Checksum" to select "Data Digest" and/or "Header Digest". Then Click "Next".

5. Enter the username and password for "Use CHAP authentication" and/or "Mutual CHAP" and click "Next". Check "Use CHAP authentication" and only the initiator is authenticated by the iSCSI target, and users of the initiators are required to enter the username and password specified here to access the target. Check "Mutual CHAP" for two-way authentication between the iSCSI target

and the initiator. The target authenticates the initiator using the first set of username and password. The initiator authenticates the target using the "Mutual CHAP" settings.

6. Click "Next".

7. Click "Finish".

8. A new target will be created.

Creating iSCSI LUNs

Follow the steps below to create a LUN for an iSCSI target:

1. Click "Create".

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

3. Configure the following settings:

- LUN type

- LUN allocation method

- Name

- LUN location

- Capacity

- Alert threshold

4. Click "Next".

5. Optional: Map the LUN to a target and click "Next".

Important: Selecting "Do not map it to a target for now" adds the newly created LUN to the unmapped iSCSI LUN list. You can add LUNs in this list to the iSCSI Target list at any time.

6. Confirm the settings and click "Next".

7. Click "Finish".

The unmapped LUN is created and listed in the unmapped iSCSI LUN list.

The description of each iSCSI target and LUN status is explained in the table below:

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

		visible to authenticated initiators.
	Disabled	The LUN is inactive and is invisible to the initiators.

Refer to the table below for actions (the "Action" button) available to manage iSCSI targets and LUNs:

Action	Description
Deactivate	Deactivate a ready or connected target. Note that the connection from the initiators will be removed.
Activate	Activate an offline target.
Modify	Modify the target settings: target alias, CHAP information, and checksum settings. Modify the LUN settings: LUN allocation, name, disk volume directory, etc.
Delete	Delete an iSCSI target. All the connections will be removed.
Disable	Disable a LUN. All the connections will be removed.
Enable	Enable a LUN.
Un-map	Un-map the LUN from the target. Note that a LUN must first be disabled before it can be un-mapped. When clicking this button, the LUN will be moved to the un-mapped iSCSI LUN list.
Map	Map the LUN to an iSCSI target. This option is only available on the un-mapped iSCSI LUN list.
View Connections	View the connection status of an iSCSI target.

Note: Some of the above options are not available if the iSCSI target is connected.

Switching iSCSI LUNs between targets

Follow the steps below to switch an iSCSI LUN between targets:

1. Select an iSCSI LUN to un-map from its iSCSI target.
2. Click "Action" > "Disable".
3. Click "OK".
4. Click "Action" > "Un-map" to un-map the LUN. The LUN will appear on the un-mapped iSCSI LUN list.
5. Select the un-mapped iSCSI LUN.
6. Click "Action" > "Map" to map the LUN to another target.

7. Select the target to map the LUN and click "Apply".
8. The LUN will be mapped to the target.

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

Expanding iSCSI LUN capacity

The NAS supports capacity expansion for iSCSI LUNs. To do so, follow the steps below:

1. Locate an iSCSI LUN on the iSCSI target list.
2. Click "Action" > "Modify".
3. Specify the capacity of the LUN. Note that the LUN capacity can be increased several times up to the maximum limit but cannot be decreased.
4. Click "Apply" to save the settings.

> **Note:** For the type of LUN allocation, the maximum LUN capacity for both thin provisioning and instant allocation is 144TB or 250TB if the NAS has more than 4GB RAM.

Optimizing iSCSI Performance

In environments that require high performance storage (virtualization, etc) users are recommended optimize the iSCSI and NAS hard disks performance in the following ways:

- **Use instant allocation:** When creating an iSCSI LUN, select "Instant Allocation" to achieve slightly higher iSCSI performance. However, the benefits of thin provisioning will be lost.
- **Create multiple LUNs:** Create multiple LUNs according to the number of processors on the NAS (this can be found in "System Status" > "Resource Monitor"). If the NAS has four processors, it is recommended to create four or more LUNs to optimize iSCSI performance.
- **Use different LUNs for heavy load applications:** Spread applications such as databases and virtual machines that need high read/write performance to different LUNs. For example, if there are two virtual machines which intensively read and write data on LUNs, it is recommended to create two LUNs so that the VM workloads can be efficiently distributed.

Advanced ACL

With the iSCSI advanced access control list (ACL), LUN masking policies can be configured for each connected initiator. If the connected initiator is not on the list, the "Default" policy will be applied to that initiator.

> **Note:** This function or its content is only applicable to some models. To check for

To use this feature, click "Add a Policy". Enter the policy name and the initiator IQN, assign the access right for each LUN created on the NAS and click "Apply".

For descriptions on each field, refer to the table below:

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

If no LUN masking policy is specified for a connected iSCSI initiator, the default policy will be applied. The system default policy allows read and write access from all the connected iSCSI initiators. Click the default policy and "Edit" to edit the default policy. To delete a policy, select a policy and click "Delete".

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

Hint: How do I find the initiator IQN?
Start the Microsoft iSCSI initiator and click "General". You can then find the IQN of the initiator.

Snapshot

QNAP Snapshot can be used with iSCSI LUNs and volumes in a QNAP NAS to achieve full protection. With the QNAP Snapshot Agent, the NAS provides application-consistent snapshots by capturing all data in memory and all transactions in process before performing the snapshot. The application will then be consistent and include all necessary data. In case of snapshot restoration, no data will be missing.

On this page, you can take, manage, or restore application (or crash consistent) snapshots on block-based LUNs or check a list of servers with Snapshot Agent installed and set up remote snapshot replication jobs.

Note:

Taking a Snapshot

After reserved space is set, you can take snapshots. To create a snapshot, follow these steps:

1. Select a LUN from the list and click "Snapshot" > "Take a Snapshot".
2. Specify the snapshot name and duration to retain the snapshot.
3. Select between Crash-consistent or application-consistent snapshot types.
4. Click "OK".

Note: Application-consistent snapshots capture all of the data from both volatile (RAM) and persistent storage (hard drives). Crash-consistent snapshots only capture the data from persistent storage. When restoring an application-consistent snapshot for a VM, all of the data (including data stored in volatile storage) will be restored. When restoring a crash-consistent snapshot, only data stored in the persistent storage will be restored.

- For Windows-based VMs, the application will need to support VSS and VSS Writer in order to take an application-consistent snapshot.
- The options ("Application-consistent" and "Crash-consistent") will only appear after you install QNAP Snapshot Agent (this can be downloaded from the QNAP website). If this is not installed, all of the snapshots taken will be crash-consistent snapshots.

Managing Snapshots

You can revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files for LUNs or volumes. For more information on these functions, see Managing Snapshots with Snapshot Manager for volumes and LUNs.

Snapshot Agent

QNAP Snapshot Agent supports VMware vCenter and Microsoft Volume Shadow Copy Service (VSS). Before taking snapshots from the NAS, the Snapshot Agent notifies vCenter or Microsoft Server to create VMware snapshots for each virtual machine and store those VMware snapshots to iSCSI LUNs (or to flush all the data into the iSCSI LUN,) thereby ensuring application consistent snapshots.

To check connected servers with Snapshot Agent installed, click "Snapshot" > "SnapAgent". On the SnapAgent page, you can check the agent IP, agent version, OS, LUN information, and status. Check www.qnap.com for details on Snapshot Agent.

Connecting to iSCSI Targets by Microsoft iSCSI Initiator on Windows

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

ISCSI initiator on Windows:
Microsoft iSCSI Software Initiator is an official application for Windows that allow users to implement an external iSCSI storage array over the network.

Using iSCSI initiator:
Start the iSCSI initiator from "Control Panel" > "Administrative Tools". Under the "Discovery" tab click "Add Portal" (or "Discover 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 want to connect to and click "Connect". You can click "Advanced" to specify login information if you have configured the authentication otherwise simply click "OK" to continue. Upon logging in, the status of the target will show "Connected".

After the target has been connected Windows will detect its presence and treat it as if a new hard disk drive has been added which needs to be initialized and formatted before we can use it. Go to "Control Panel" > "Administrative Tools" > "Computer Management" > "Disk Management" and you should be prompted to initialize the newly-found hard drive. Click "OK" then format this drive as you normally 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.

Connecting to iSCSI Targets by Xtend SAN iSCSI Initiator on Mac OS

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

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

Using Xtend SAN iSCSI initiator:
Follow the steps below:
1. After installing the Xtend SAN iSCSI initiator, you can find it in "Applications".
2. Click the "Discover Targets" tab and choose "Discover by DNS/IP" or "Discover by iSNS" according to the network topology. In this example, we will use the IP address to discover the iSCSI targets.
3. Follow the instructions and enter the server address, iSCSI target port number (default: 3260), and CHAP information (if applicable). Click "Finish" to retrieve the target list.
4. The available iSCSI targets on the NAS will be shown. Select the target you want to connect to and click "Add".

You can configure the connection properties of selected iSCSI target in the "Setup" tab. Click the "Status" tab, select the target to connect to. Then click "Login" to proceed. The first time you login to the iSCSI target, a message will remind you the disk is not initialized. Click "Initialize…" to format the disk. You can also open "Disk Utilities" to initialize the disk. You can now use the iSCSI target as an external drive on your Mac.

Connecting to iSCSI Targets by Open-iSCSI Initiator on Ubuntu Linux

This section shows you how to use the Linux Open-iSCSI Initiator on Ubuntu to add the iSCSI target as an extra partition. Before you start using 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 (and 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, visit: http://www.open-iscsi.org

> **Note:** Snapshot LUNs are not supported by the Linux Open-iSCSI Initiator.

Using Linux Open-iSCSI Initiator:

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

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

Follow these steps to connect to an iSCSI target 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, 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 nodes to connect.

```
# iscsiadm -m node
```

** You can delete the nodes you do not want to connect to when the service is on with the following command:

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

Restart open-iscsi to login all the available nodes.

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

You should be able to see the login message as below:

Login session [iface: default, target: iqn.2004-04.com:NAS:iSCSI.ForUbuntu.B9281B, portal: 10.8.12.31,3260] [OK]

Check the device status with dmesg.

`# dmesg | tail`

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

`# fdisk /dev/sdb`

Format the partition.

`# mkfs.ext3 /dev/sdb1`

Mount the file system.

`# mkdir /mnt/iscsi`

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

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

`# hdparm -tT /dev/sdb1`

Below are some "iscsiadm" related commands.

Discover the targets on the host:

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

Login a target:

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

Logout a target:

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

Delete a Target:

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

LUN Backup

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

In this chapter, these topics are covered:

- Backing up iSCSI LUNs
- Restoring iSCSI LUNs
- Creating iSCSI LUN Snapshots
- Managing LUN Backup/Restore/Snapshot by Command Line

> **Note:** This function or its content is only applicable on some models. To check for applicable models, please refer to the   product comparison table on the QNAP website.
> - A minimum of 4 GB RAM is required to use snapshots.
> - x51 series models only support up to 256 snapshots instead of 1024. The HS-251 does not support snapshots.

Backing up iSCSI LUNs

The entire LUN can be backed up as an image file and saved to a different location. The storage location can be a Windows share (SMB/CIFS), a Linux share (NFS), or a local folder on the NAS.

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

1. Click "Create a job".
2. Select "Back up an iSCSI LUN" and click "Next".
3. Select the source LUN for backup. If an online LUN is selected, the NAS will automatically create a point-in-time snapshot for the LUN.
4. Specify the destination where the LUN will be backed up to. The NAS supports LUN backup to a Linux share (NFS), a Windows share (CIFS/SMB), and a local folder on the NAS. Click "Test" to test the connection to the specified path. Then click "Next".
5. Enter a name of the backup LUN image or use the one generated by the NAS. Select the subfolder where the image file will be stored. Select to use compression or not and click "Next". (Use Compression: When this option is enabled, more CPU resources of the NAS will be used but the size of the backup LUN can be reduced. The backup time may vary depending on the size of the iSCSI LUN.)

6. Specify the backup schedule, choose the backup period (Now, Hourly, Daily, Weekly, or Monthly) and click "Next".
7. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next."
8. Click "Finish" to exit.
9. The backup job is shown on the list.

Refer to the table below for actions (the "Action" button) available to manage the backup jobs.

Action	Description
Edit	Edit the job settings.
Delete	Delete the job.
Start	Start the job immediately.
Stop	Stop the running job.
View Logs	View the job status and logs.

Restoring iSCSI LUNs

A LUN image can be restored to the NAS. Users can choose to overwrite the original LUN or create a new one by renaming the LUN. To restore an iSCSI LUN to the NAS, follow these steps:

1. Go to "Storage Manager" > "LUN Backup". Click "Create a job".
2. Select "Restore an iSCSI LUN" and click "Next."
3. Specify the protocol, IP address/host name, and folder/path of the restore source. Click "Test" to test the connection. Then click "Next".
4. Browse and select the LUN image file and click "Next."
5. Select the destination and click "Next".
6. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next".
7. Click "Finish" to exit.

The restore job will be executed immediately.

Refer to the table below for actions (the "Action" button) available to manage restore jobs.

Action	Description
Edit	Edit the job settings.
Delete	Delete the job.
Start	Start the job immediately.
Stop	Stop the running job.
View Logs	View the job status and logs.

Note: For Step 5 above:
- Overwrite existing LUN: Restore the iSCSI LUN and overwrite the existing LUN on the NAS. All the data on the original LUN will be overwritten.
- Create a new LUN: Restore the iSCSI LUN to the NAS as a new LUN. Enter the name and select the location of the new LUN. Make sure you have created at least one LUN on the NAS before editing the default LUN policy.

Creating iSCSI LUN Snapshots

A read-only LUN snapshot can be created and mounted to an iSCSI target on the NAS for data access from other hosts or LUN backup. The contents of the LUN snapshot will remain the same regardless of the changes made to the original LUN. Before creating an iSCSI LUN snapshot, make sure at least one iSCSI LUN and one iSCSI target has been created on the NAS.

To create an iSCSI LUN snapshot, follow these steps:
1. Go to "Storage Manager" > "LUN Backup". Click "Create a job".
2. Select "Create a LUN Snapshot" and click "Next".
3. Select an iSCSI LUN on the NAS. Only one snapshot can be created for each iSCSI LUN. Click "Next".
4. Enter a name for the LUN snapshot or use the one generated by the NAS. Select an iSCSI target where the LUN snapshot is mapped to. Click "Next". The LUN snapshot must be mapped to another iSCSI target different from the original one.
5. Specify the snapshot schedule and the snapshot duration and click "Next". The snapshot will be automatically removed when the snapshot duration is reached.
6. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next".
7. Click "Finish" to exit.
8. The snapshot will be created immediately. The status and duration will be shown on the list.

9. Go to "Storage Manager" > "iSCSI Storage", and the snapshot LUN will be shown in the iSCSI Target List. Use iSCSI initiator software to connect to the iSCSI target and access the point-in-time data on the snapshot LUN.

Note: The source LUN and snapshot LUN cannot be mounted on the same NAS or certain operating systems such as Windows 7 and Windows 2008 R2. In this case, mount the LUN snapshot to a different NAS or server.

Managing LUN Backup/Restore/Snapshot by Command Line

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

1. First make sure the iSCSI LUN backup, restore, or snapshot jobs have been created on the NAS in "Storage Manager" > "LUN Backup".
2. Connect to the NAS by an SSH utility such as Putty.
3. Login the NAS as an administrator.
4. Input the command "lunbackup". The command usage description will be shown.
5. Use the lunbackup command to start or stop an iSCSI LUN backup, restore, or snapshot job on the NAS.

Note: The above procedure should only be carried out by administrators who are familiar with command line interfaces.

Virtual Disk

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

Supported file systems:

Format: Ext3, Ext4, FAT, NTFS, and HFS+.

Mount: Ext3, Ext4, FAT, NTFS, and HFS+.

> **Note:**
> - The NAS supports a virtual disk with a maximum size of 16TB.
> - When a virtual disk (iSCSI target) is disconnected, the virtual disk will disappear from the interface and the NAS will try to connect to the target in 2 minutes. If the target cannot be connected to after 2 minutes, the status of the virtual disk will become "Disconnected".
> - Each virtual disk drive will be recognized as a single logical volume by the local system.
> - This function is only applicable to some models. To check for applicable models, please refer to the product comparison table on the QNAP website.

To add a virtual disk to the NAS, follow the steps below:

1. Make sure an iSCSI target has been created. Go to "Storage Manager" > "Remote Disk" and click "Add Virtual Disk".
2. Enter the target server IP and port number (default: 3260). Click "Get Remote Disk" and select a target from the target list. If authentication is required, enter the username and the password. Select the options "Data Digest" and/or "Header Digest" (optional). These are the parameters for which the iSCSI initiator is verified when it attempts to connect to the iSCSI target. Then, click "Next".
3. Enter a name for the virtual disk. If the target is mapped with multiple LUNs, select a LUN from the list. Make sure that only this NAS can connect to the LUN. The NAS supports mounting EXT3, EXT4, FAT32, NTFS, HFS+ file systems. If the file system of the LUN is "Unknown", select "Format virtual disk now" and choose the file system. You can format the virtual disk as EXT3, EXT4, FAT 32, NTFS, or HFS+. By selecting "Format virtual disk now", the data on the LUN will be cleared. Then, click "Next".
4. Click "Finish".
5. The storage capacity of the NAS is expanded by the virtual disk. Users can go to "Privilege Settings" > "Share Folders" to create new shared folders on the virtual disk.

Refer to the table below for actions (the "Action" button) available to manage virtual disks:

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

External Device

You can use an external device as a virtual disk. Check the External Device chapter for details.

Security

Go to "Control Panel" > "System" > "Security" to configure relevant security settings for your NAS.
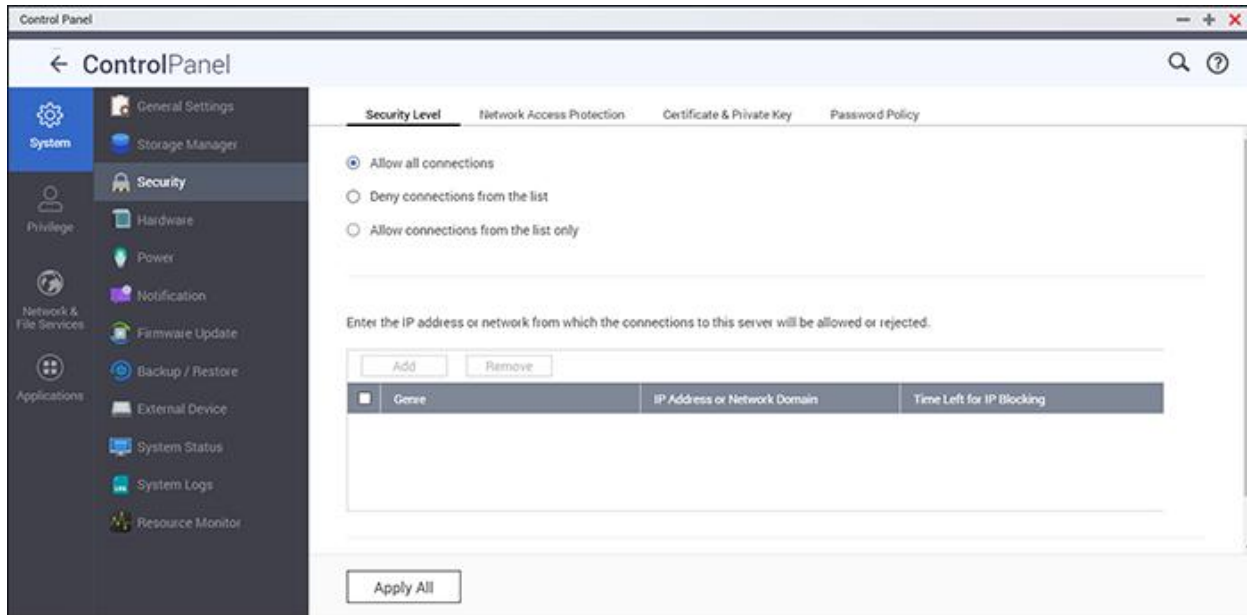
Security Level

Specify the IP address or network domain from which connections to the NAS are allowed or denied. When the connection of a host server is denied, all the protocols of that server are not allowed to connect to the NAS. After changing the settings, click "Apply" to save the changes. Network services will be restarted and current connections to the NAS will be terminated.

Network Access Protection

Network access protection enhances system security and prevents unwanted intrusion. You can block an IP address for a certain period of time or indefinitely if the IP address fails to login to the NAS using a particular connection method (e.g. SSH, Telnet, HTTPS, FTP, SAMBA, or AFP).

Certificate & Private Key

Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload an SSL certificate issued by trusted providers. After uploading an SSL certificate, users can connect to the administration

interface of the NAS by SSL and there will not be any alert or error message. The NAS only supports X.509 certificates and private keys.

- Replace Certificate: Upload a new certificate from a trusted provider, create a self-signed certificate, or get one from the open certificate authority "Let's Encrypt".
- Download Certificate: Download the secure certificate which is currently in use.
- Download Private Key: Download the private key which is currently in use.
- Restore Default Certificate & Private Key: Restores the secure certificate and private key to system default. The secure certificate and private key in use will be overwritten.

Note: This option is only available after the default certificate has been replaced.

Password Policy

Password policy allows the administrator to set the minimum password strength of user passwords and to force users to change their passwords periodically.

Password Strength

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

- A new password must contain characters from at least three of the following types of characters: lowercase letters, uppercase letters, digits, and special characters.
- No character in the new password may be repeated more than three consecutive times.
- The new password must be different than the username and must not be the username reversed.

Force Password Change

The administrator may force users to change their passwords periodically by setting the number of days before a password expires. There is also an option to email users a week in advance of their password expiring.

Hardware

Go to "Control Panel" > "System Settings" > "Hardware" to configure the NAS hardware functions.

In this chapter, the following topics are covered:

- General Settings (General)
- Audio Alert
- Smart Fan

General Settings (General)

- **Enable configuration reset switch:** When this is enabled, you can press the reset button for 3 seconds to reset the administrator password and the system settings to default (NAS data will be retained) or 10 seconds for advanced system reset.
  - ○ **Basic system reset:** You will hear a beep after pressing and holding the reset button. 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: Disables Jumbo Frames.
    - ▪ TCP/IP configuration: If port trunking is enabled, the port trunking mode will be reset to "Active Backup (Failover)".

- System port: 8080 (system service port.)
- Security level: Low (Allows all connections.)
- LCD panel password: (blank); this feature is only for NAS models with LCD panels.
- VLAN will be disabled.
- Service binding: All NAS services will be run on all available network interfaces.
  - **Advanced system reset:** You will hear two beeps after continuously pressing the reset button. The NAS will reset all system settings to default (similar to the system reset in "Administration" > "Restore to Factory Default") except all the NAS data will be reserved. Settings such as users, user groups, and shared folders will be cleared. To retrieve old data after an advanced system reset, create the same shared folders on the NAS and the data will be accessible again.
- **Enable hard disk standby mode:** This option allows the NAS drives to enter standby mode if there is no disk access within the specified period. Note that during standby mode, the system LED on the NAS will be off but the HDD status LED will remain steady.
- **Enable light signal alert when the free size of SATA disk is less than the value:** The status LED will flash red and green if this option is enabled and the free space of the SATA hard drive is less than the set value.
- **Enable write cache (EXT4 only):** If the NAS disk volume uses EXT4, enable this option for higher write performance. Note that an unexpected system shutdown may lead to data loss. It is recommended to disable this option if the NAS is set as shared storage in a virtualized or clustered environment.
- **Enable warning alert for redundant power supply on the web-based interface:** If two power supply units (PSU) are installed on the NAS and connected to the power sockets, both PSU will supply the power to the NAS (applied to 1U and 2U models.) Turn on the redundant power supply mode in "System Settings" > "Hardware" to receive warnings for the redundant power supply. The NAS will sound and record error messages in "System Logs" if the PSU is plugged out or does not respond correctly. If only one PSU is installed on the NAS, DO NOT enable this option. This function is disabled by default.
- **Turn on LED light:** If your NAS has a LED indicator (ex. TS-453mini), you can choose to turn on its LED indicator, set the LED brightness level and configure a schedule for the brightness setting. This function is only applicable on some models.

Audio Alert

You can configure the buzzer or speaker alarm for system operations and events. The following options are available:

- System operations: The system beeps or announces messages when system operations such as booting and firmware updates occur.
- System events: The system beeps or announces error or warning messages for system events.

- Enable speech notification: Beeping sounds for certain events are replaced by speech. You can also choose the audio language and adjust the volume. If this feature is not enabled, the system only beeps when system operations are executed and when system events occur.
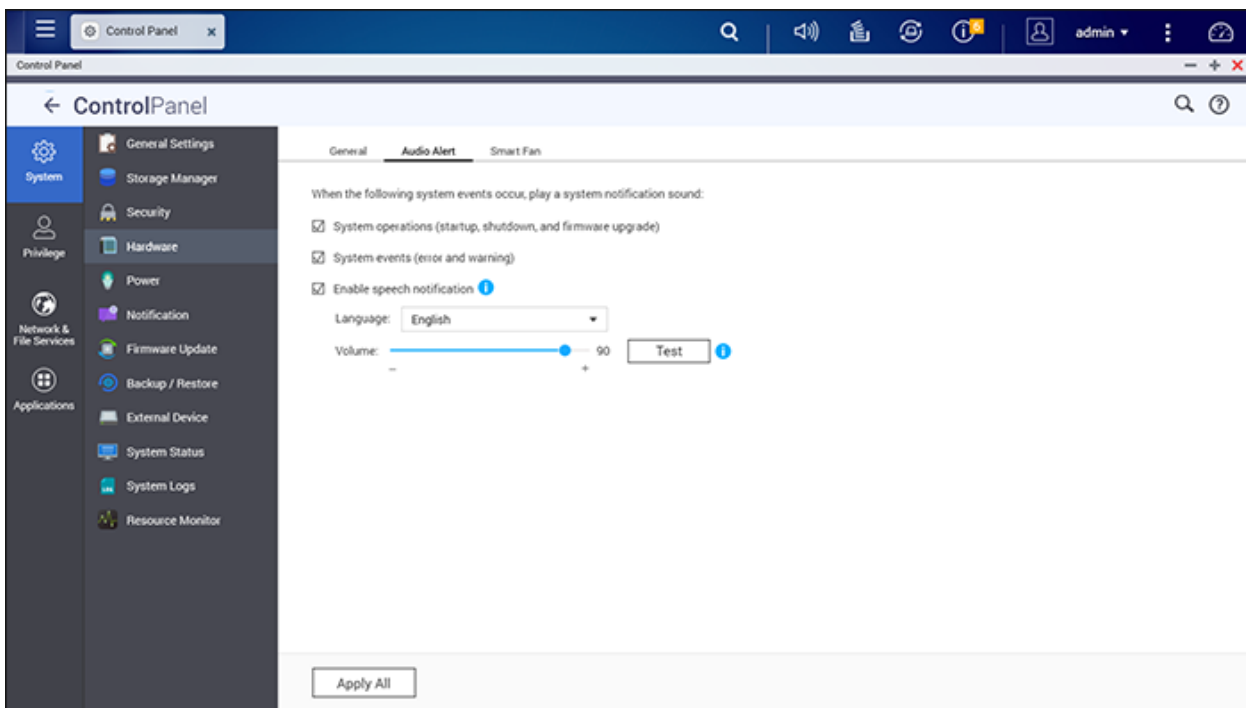
> **Note:**
> - Speech notification is only available for certain NAS models. Refer to the official QNAP website for details.
> - Speech notification messages will not be played if the built-in speaker (available only on certain NAS models) is being used by another app (such as the Music Station player).
> - If event B occurs while the system is still announcing an audio message for event A, the system will not announce event B.

QTS provides the following audio messages:
- Audio test
- Completed RAID initialization or rebuilding
- Disk plugged in
- Disk unplugged
- Fan module error
- Firmware update completed
- Hard drive not recognized. Please replace it.
- Initializing or rebuilding RAID
- iSCSI LUN has reached the threshold

- JBOD plugged in
- JBOD unplugged
- Power error
- Power failure
- Processing USB ejection
- Restarting HD Station
- Restating Linux Station
- Running advanced system reset
- Running USB one touch copy
- Shutting down
- Starting HD Station
- Starting Linux Station
- Storage Pool error
- Storage Pool has reached the threshold
- Storage Pool is full
- System boot completed
- Thunderbolt device has been connected.
- Thunderbolt device has been disconnected.
- Testing system
- Updating firmware now, please do not turn off the power
- USB backup completed
- Volume has reached the threshold
- Volume is full
- You can now safely remove your USB device

> **Important:** The volume control on the Audio Alert screen adjusts only the volume for audio messages, while the volume control on the QTS desktop controls the volume for sounds other than audio messages. For example, you will hear audio messages if the volume on the Audio Alert screen is set to the maximum and the volume on the QTS desktop is muted.

Smart Fan

After enabling Smart Fan, the fan rotation speed will be automatically adjusted according to the NAS temperature and you can define the temperature settings to increase or decrease the fan rotation speed. By manually setting the fan rotation speed, the fan will continuously rotate at the defined speed. The following settings are available:
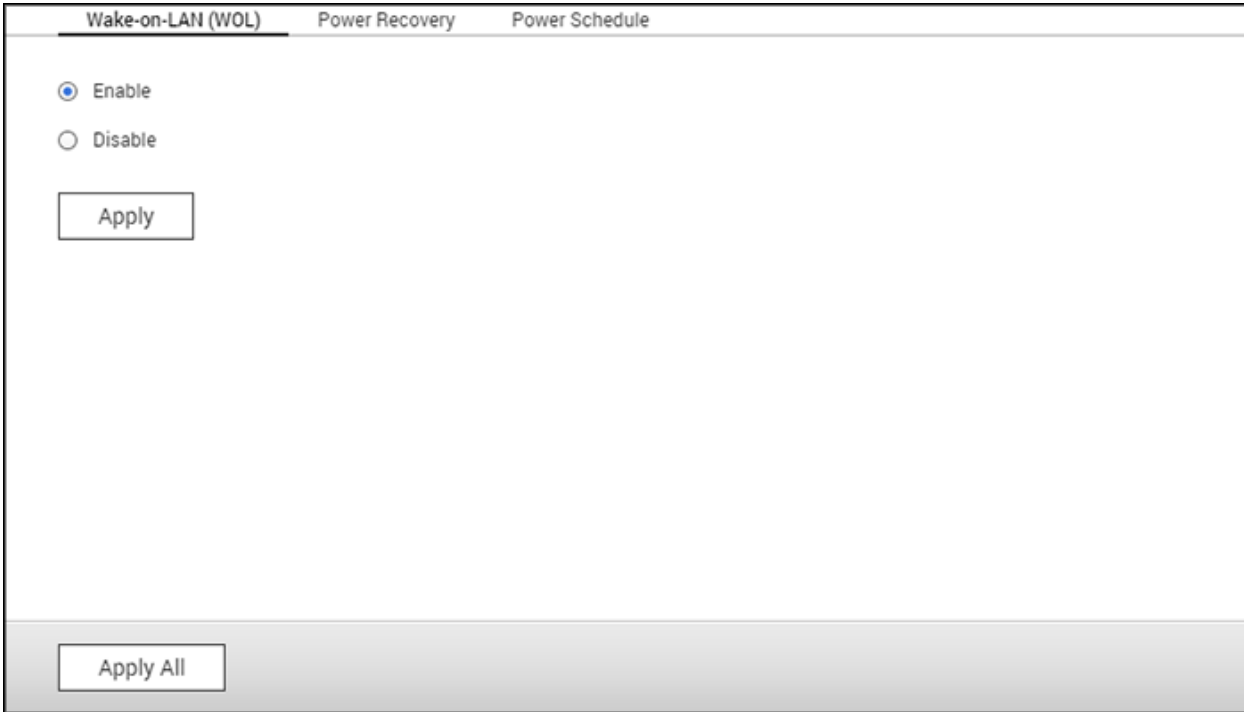
- Enable smart fan (recommended): Select to use the default smart fan settings or to manually define the temperature settings. For the default smart fan settings, the system will self-monitor the CPU temperatures and automatically adjust the fan speed accordingly. You can also set three self-defined settings to either maintain the temperature at certain level, to run the fan at the lowest speed, or to run the fan at the highest speed if the temperature reaches a temperature setting.
- Set fan rotation speed manually: By manually setting the fan rotation speed, the fan will continually rotate at this speed.

> **Note:**
> - For NAS models with multiple fans, you can individually set the fans for the system block and CPU block. For these models, there are three fan modes available for the system block:
>   - Quiet mode: In this mode, the fan will rotate at the lowest possible speed to minimize noise.
>   - Normal mode: In this mode, the system will adjust the fan speed intelligently and automatically.
>   - Performance mode: In this mode, the fan will rotate at the highest possible speed to reduce the system temperature.
> - The NAS will automatically shut down to protect itself if a temperature threshold is exceeded. The threshold values vary depending on NAS models.

Power

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

| Wake-on-LAN (WOL) | Power Recovery | Power Schedule |

⦿ Enable

○ Disable

Apply

Apply All

EuP Mode Configuration

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

When EuP is enabled, the following settings will be affected so that the NAS maintains low power consumption (less than 1W) when the NAS is powered off:
- Wake on LAN: Disabled.
- AC power resumption: The NAS will remain off after the power restores from an outage.
- Scheduled power on, off, restart settings: Disabled.

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

This feature is only supported by certain NAS models.

Wake-on-LAN (WOL)

Enable this option to allow users to power on the NAS remotely by Wake on LAN. If the power cable is unplugged when the NAS is turned off, Wake on LAN will not function even if the power supply is reconnected afterwards. To wake up the NAS when it is in sleep mode or powered down, press the NAS power button or use the WOL feature in Qfinder Pro or Qmanager. The wake-up function on the NAS is only available after the WOL option is enabled in "Control Panel" > "System Settings" > "General Settings" > "Power" > "Wake-on-LAN (WOL)".

- For Qfinder Pro, select a NAS and click "Tools" > "Remote Wake Up (Wake on LAN)".
- For Qmanager, click ">" next to the NAS to be selected on the login page, scroll down to the bottom of the screen and click "Wake on LAN (WOL)".

This feature is only supported by certain NAS models.

Power Recovery

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.

> **Note:** Only x86-based NAS models can be turned on automatically after power recovery. To set it up, select "Turn on the server automatically" in "Control Panel" > "System Settings" > "Power" > "Power Recovery".

Power Schedule

Specify the schedule for automatic system power on/off, restart, or sleep mode. Weekdays are Monday to Friday, weekends are Saturday and Sunday. Up to 15 schedules can be set.
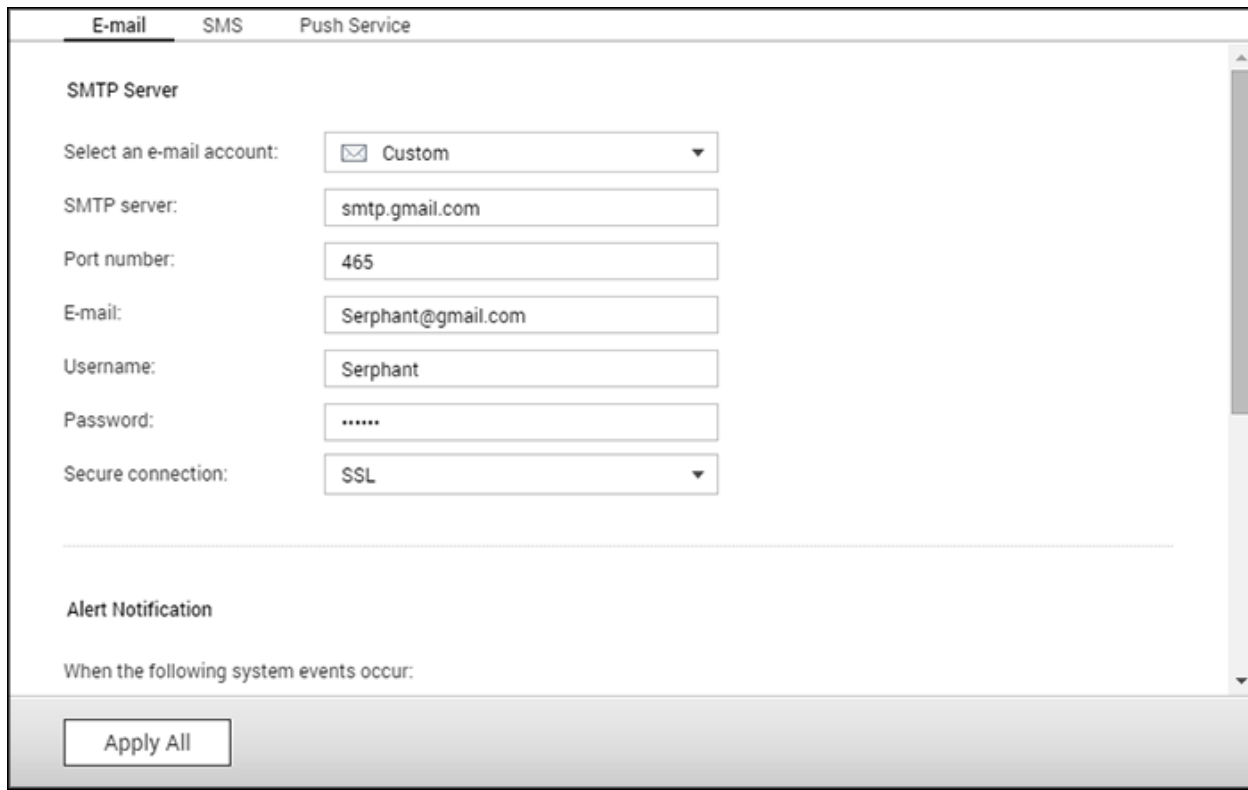
Enable "Postpone the sleep/restart/shutdown schedule when replication job is in process" to allow scheduled system restart/shutdown to be carried out after a running replication job completes. Otherwise, the NAS will ignore the running replication job and execute scheduled system restart or shutdown.

> **Note:**
> - The system cannot be shut down or restarted in sleep mode.
> - If there are other QNAP storage expansion enclosures connected to the NAS, the sleep mode will be disabled automatically and system will not go into sleep mode.

Notification

Go to "Control Panel" > "System Settings" > "Notification" to configure NAS notifications.

E-mail

The NAS can send email messages to specified recipients using an assigned service provider or SMTP server.

Configuring Email Notifications

1. Go to "Control Panel" > "System Settings" > "Notification" > "Email".
2. Under "SMTP Server", configure the following settings:
- Select an email account: Select the service provider to be used for sending email notifications.

> **Note:** If the service provider is not listed, select "Custom" and configure the following settings:
> o SMTP server: Type the server name (for example, "smtp.example.com").
> o Port number: Type the port number to be used for connections. The default port number is 25.

- E-mail: Type the email address of the sender account.
- Password: Type the password for the sender account.
3. Under "Alert Notification", perform the following steps:
4. Click "Apply".

SMS

The NAS can send SMS messages to specified mobile numbers using an assigned service provider or SMSC server.

Configuring SMS Notifications

1. Go to "Control Panel" > "System Settings" > "Notification" > "SMS".
2. Under "SMSC Server", configure the following settings:
a. Specify the service provider to be used for sending SMS notifications. QTS provides the following options:
○ SMS service provider: Type the service provider name (for example, "Clickall").
○ URL template text:

b. Optional: If the SMSC server supports secure connections, select "Enable SSL connection" and specify the required server information.
3. Under "Alert Notification", perform the following steps:
a. Select the types of system events that should trigger email alerts.
- Error: An error that requires your attention has occurred.
- Firmware Update: A new firmware version is available for download and installation.
b. Select a country code and specify at least one recipient mobile number.
c. Optional: Click "Send a Test SMS Message" to verify the SMSC server settings.
4. Click "Apply".

Push Service

The push service allows you to receive notifications in the following locations whenever warning or error events occur.

- Web browsers: Notifications display even if the QTS window is not open. QTS supports the latest versions of Google Chrome and Apple Safari.
- Mobile devices: Notifications display if Qmanager is installed and the device is paired with the NAS.

Configuring Push Notifications

1. Log on to myQNAPcloud.
2. Select the types of notifications that you want to receive.
3. Install one of the following Qmanager versions on your mobile device:
- Qmanager iOS 1.8.0
- Qmanager Android 2.1.0 or later
4. Log on to the NAS using Qmanager and confirm to receive push notifications.

> **Note:** You can also disable this service on Qmanager by clicking ">" next to a NAS connection and then modifying the push service properties on the "server settings" screen.

5. To enable notifications on the current browser, click "Pair" and then perform the following steps.
a. In the pop-up message that appears, Click "Allow".
b. Optional: Edit the default browser name and then click "Apply".

The system pairs the device with the NAS and displays device information in the "Set up paired devices" table.

> **Note:** unpair devices from the NAS and disable browser notifications, perform one of the following steps:
> - In the "Browser" section, click "Unpair".
> - In the "Set up paired devices" table, select the device and then click "Remove device".

6. Select the types of system events that should trigger push notifications.
7. Verify that the paired devices are listed in the "Manage Paired Devices" table.

The NAS will send alert notifications to paired mobile devices whenever a relevant event occurs. You can disable or delete a paired device from the table.

> **Note:** Some notifications may not be displayed immediately because of iOS and Android server issues.

Firmware Update

Go to "Control Panel" > "System Settings" > "Firmware Update" to update the firmware version of the NAS.

Live Update

Select "Automatically check if a newer version is available when logging into the NAS web administration interface" to allow the NAS to automatically check if a new firmware version is available. If a new firmware is found, you will be notified after logging in the NAS as an administrator. Click "Check for Update" to check if any firmware update is available. Note that the NAS must be connected to the Internet for these features to work.

> **Note:** Experience the latest apps and features for QNAP NAS by joining our beta programs. You can join by checking "Join the QTS Beta program to receive beta update notifications".

Firmware Update

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

1. Download the firmware release notes from the QNAP website http://www.qnap.com. Read the release notes carefully to make sure it is necessary to update the firmware.
2. Download the NAS firmware and unzip the IMG file to the computer.

3. Before updating the system firmware, back up all the NAS data to avoid any potential data loss from unforeseen issues arising during the system update.
4. Click "Browse" to select the firmware image for the system update. Click "Update System" to update the firmware.

The system update may take seconds, minutes or longer to complete depending on the network connection status. The NAS will inform you when the system update has completed.

> **Note:**
> - If the system is running properly, you do not need to update the firmware.
> - QTS does not support downgrading the firmware. However, if you choose to apply an older firmware version, please back up all of your important data before downgrading. QNAP is not responsible for any damage to the NAS or its contents after downgrading.

Update Firmware by QNAP Qfinder Pro

The NAS firmware can be updated using Qfinder Pro by following these steps:
1. Select a NAS model and choose "Update Firmware" from the "Tools" menu.
2. Login to the NAS as an administrator.
3. Browse and select the firmware for the NAS. Click "Start" to update the system.

> **Note:** If you have multiple identical NAS on the same LAN, they can be updated at the same time with Qfinder Pro. Administrator access is required.

Backup/Restore

Go to "Control Panel" > "System Settings" > "Backup/Restore" to back up, restore your NAS or restore your NAS to factory default settings.

Backup/Restore Settings

- **Back up System Settings:** To back up all the settings, including the user accounts, server name, network configuration and so on, click "Backup" and select to open or save the setting file. Settings will be backed up include: User, Group, Shared Folder, Workgroup, Domain, and LDAP, Windows File Service, Mac File Service, NFS, FTP, WebDAV, Network Backup, User Home, Password Settings, SNMP, and Backup Service.
- **Restore System Settings:** To restore all the settings, click "Browse" to select a previously saved setting file and click "Restore".

Note:
- User Home includes basic service settings (excluding user data in the user home folder.)
- If the users or groups you try to restore from the backup file already exist in the current system, the users and groups in the current system will be overwritten.

Restore to Factory Default

- **Restore Factory Defaults & Format all Volumes:** Restore system settings to default and **formats all disk volumes**.
- **Reset Settings:** Restore system settings to default without erasing user data.
- **Reinitialize NAS:** **Erases all data** and reinitializes the NAS.

Caution: The administrator's password and system settings will be reset to default if you press and hold the reset button on the back of the NAS for 3 seconds (data and files on the NAS will be unaffected.) However, if you press and hold the Reset button for 10 seconds, all settings including users, user groups, and shared folders will be cleared (but user data will be unaffected.)
Note: For the above "Reset Settings" and "Reset Factory Default & Format Volume" buttons, only one of them is available on the page (depending on the NAS model.)

External Device

Go to "Control Panel" > "System Settings" > "External Storage" to configure external storage devices, USB printers and UPS systems.
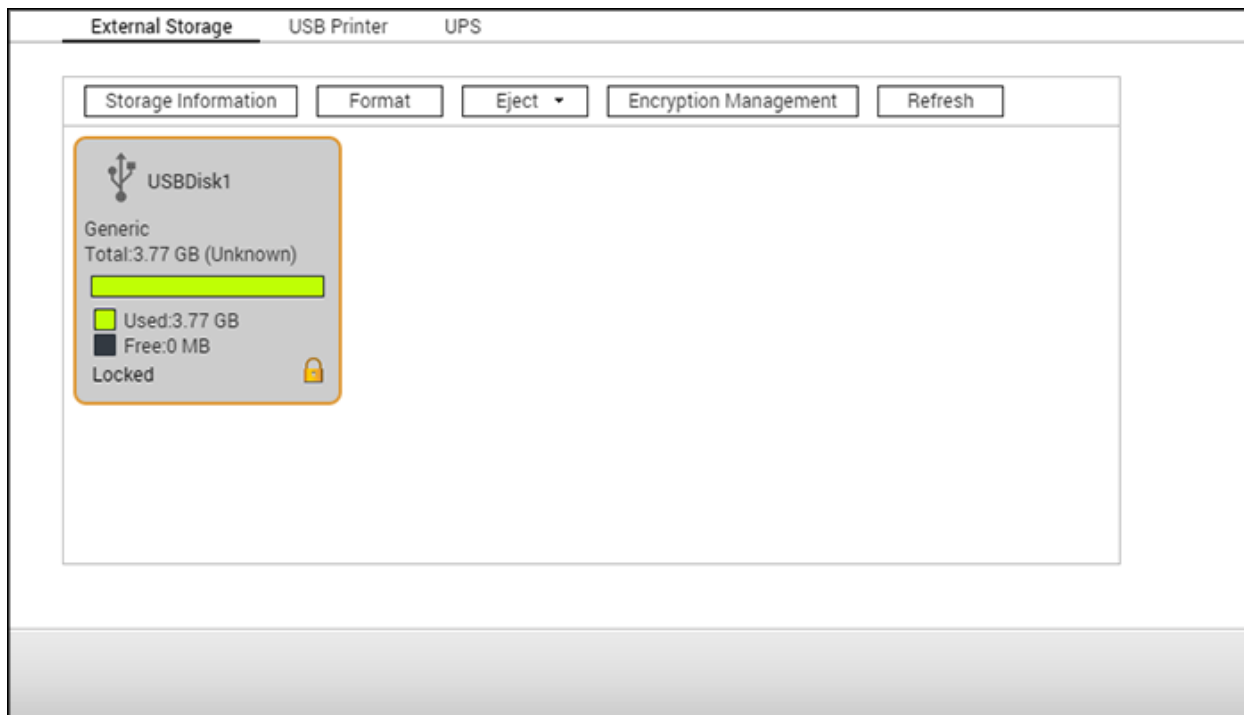
For details on these features, refer to the following links:

- External Storage
- USB Printer
- UPS

External Storage

The NAS supports USB and eSATA storage devices for backup and data storage. Connect the external storage device to a USB or an eSATA port of the NAS and its details will be shown on this page.

In this chapter, the following topics are covered:
- Storage Information
- Format
- Eject
- Encryption Management
- Data Sharing

Storage Information

Select a storage device and click "Storage Information" to check its details. The number of USB and eSATA interfaces supported varies by model. It may take a few seconds for the NAS to detect external USB/eSATA devices.

Format

External storage devices can be formatted as EXT3, EXT4, FAT32, NTFS, or HFS+ (Mac only). Click "Format" and select the option from the drop-down menu.

> **Note:** Starting with QTS 4.1, labeling is supported for external USB devices. To edit a USB drive's label, click "Storage Information" to edit its label. The label will become the shared folder name of this USB device in File Station.

The NAS supports encrypting external drives. To encrypt an external storage device, click "Encryption". Select the encryption method: AES 128-, 192- or 256-bit and enter the password (8-16 characters.) Select "Save encryption key" to save the password in a hidden location on a hard drive in the NAS. The NAS will automatically unlock the encrypted external storage device when the device is connected. Click "Format" to proceed. Click "OK" and all the data will be cleared. The device will be "Ready" after disk initialization.

> **Note:** We recommend formatting disk volumes larger than 2TB using EXT4, NTFS, or HFS+.

Eject

"Eject" offers two different options. "Disconnect disk partition" allows you to remove a single disk partition or a disk drive in a multi-drive enclosure. "Remove device" allows you to disconnect external storage devices without the risk of losing any data when the device is removed. First choose a device to eject, click "Eject" and then disconnect the disk partition or remove the device.

> **Note:** To avoid potential data loss, always use the hardware removal function before removing your external storage device (for a Windows PC, use the "Safely Remove Hardware"; for a Mac, use the "Eject" icon; for QTS, use the "Eject" button.)

Encryption Management

If an external storage device is encrypted by the NAS, the button "Encryption Management" will appear. Click this button to manage the encryption password/key, or to lock/unlock the device.

Locking the device
1. To lock an encrypted external storage device, click "Encryption Management".
2. Select "Lock this device" and click "Next".
3. Click "Next" to lock the device.

> **Note:**
> - Before you encrypt an external storage device, you must format that device and select an encryption standard from the "Encryption" drop-down list in the "Format External Storage Drive" dialog.
> - External storage devices cannot be locked if a real-time or scheduled backup job is running on it. To disable the backup job, go to "Control Panel" > "Applications" > "Backup Station" > "External Drive".

Unlocking the device
1. To unlock an encrypted external storage device, click "Encryption Management".
2. Select "Unlock this device". Click "Next".
3. Enter the encryption password or upload the key file. Select "Save encryption key" to save the password in a hidden location on a hard drive of the NAS. The NAS will automatically unlock the encrypted external storage device every time the device is connected.

Managing the encryption key

1. To change the encryption password or download an encryption key file, click "Encryption Management".

2. Select "Manage encryption key". Click "Next".

3. Select to change the encryption password or download the encryption key file to the local PC.

Data Sharing

Select "Data sharing" for an external storage device connected to a 1-bay NAS.

> **Note:** HD Station will reboot when external devices are unmounted.

USB Printer

The NAS supports network printing sharing service over local networks and the Internet in Windows, Mac, and Linux (Ubuntu) environments. Up to 3 USB printers are supported.

To share a USB printer, connect the printer to a USB port on the NAS. The printer will be automatically detected and its information displayed.

Printer Info

Click on a connected USB printer and then "Printer Info" to review its details.

> **Note:**
> - Connect a USB printer to the NAS after the software configuration is completed.
> - The NAS does not support multifunction printers.
> - The file name display for the printer job table is only available for printer jobs sent via IPP (Internet Printing Protocol).
> - For a list of supported USB printers, visit http://www.qnap.com.

Printer Log

Click on a connected USB printer and then "Printer Log" to view its print job history. You can pause or cancel ongoing/pending jobs, resume paused jobs, or delete completed or pending jobs. To clear the history, click "Clear".

> **Note:** Do NOT restart the NAS or update the system firmware when printing is in process or there are queued jobs. Otherwise all the queued jobs will be cancelled and removed.

Clean Up Spool Space

Click "Clean Up Spool Space" to clean up the data saved in the printer spool.

Settings
Click "Settings" to configure basic settings of the printer.
- **Stop printer sharing and clear print spool:** Select this option to temporarily disable the selected printer for print sharing. All of the data in the printer spool will be cleared.

- **Bonjour printer support:** Select this option to broadcast printing service to Mac users via Bonjour. When naming your printer, the name can only contain "a-z", "A-Z", "0-9", dot (.), comma (,) and dash (-).

Maximum Printer Jobs and Blacklist

- **Maximum printer jobs per printer:** Specify the maximum number of printer jobs for a printer. A printer supports up to 1,000 printer jobs. The oldest printer job will be overwritten by the newest one if the printer has reached the maximum number of printer jobs.
- **Enter IP addresses or domain names to allow or deny printing access:** To allow or deny particular IP addresses or domain names from using the NAS printing service, select "Allow printing" or "Deny printing" and enter the IP addresses or domain names. An asterisk (*) denotes all connections. To allow all users to use the printer, select "No limit". Click "Apply" to save the settings.

Note: This feature only works for printing service via IPP and Bonjour, but not Samba.

Windows 7

Follow these steps to set up your printer connection:

1. Go to Devices and Printers.
2. Click "Add a printer".
3. In the Add printer wizard, click "Add a network, wireless or Bluetooth printer".
4. While Windows is searching for available network printers, click "The printer that I want isn't listed".
5. Click "Select a shared printer by name", and then enter the address of the network printer. The address is in the following format – http://NAS_IP:631/printers/ServernamePR, where the NAS_IP can also be a domain name address if you want to print remotely. For example, http://10.8.13.59:631/printers/NASPR3
6. The wizard will prompt you for the correct printer driver. You can also download the latest printer driver from the manufacturer's website if it is not built-into Windows operating system.
7. After installing the correct printer driver, the wizard shows the address and driver of the new network printer.
8. You can also set the network printer as the default printer or print a test page. Click "Finish" to exit the wizard.
9. The new network printer is now available for printing.

Mac OS 10.6

If you are using Mac OS 10.6, follow these steps to configure the NAS printer function:

1. First make sure that Bonjour is enabled on the NAS in "External Device" > "USB Printer" > "Settings". You can change the Service Name to better represent the printer.
2. On your Mac, go to "System Preferences", and then click "Print & Fax".
3. In the Print & Fax window, click + to add a printer.
4. The USB network printer will be listed via Bonjour. Select the default printer driver or download and install the latest one from the printer manufacturer's website. Click "Add" to add this printer.
5. Additional options may be available for your printer. Click "Continue".
6. The new network printer is now available for printing.

Mac OS 10.5

If you are using Mac OS X 10.5, follow these steps to configure the NAS printer function:

1. Go to "Network Services" > "Win/Mac/MFS" > "Microsoft Networking". Enter a workgroup name for the NAS. You will need this information later.
2. Go to "Print & Fax" on your Mac.
3. Click + to add a printer.
4. Select the NAS workgroup and find the printer name.
5. Enter the username and password to login the printer server on the NAS.
6. Select the printer driver.
7. After installing the printer driver correctly, you can start using the printer.

Mac OS 10.4

If you are using Mac OS 10.4, follow these steps to configure the NAS printer function:

1. On the toolbar, click "Go/Utilities".
2. Click "Printer Setup Utility".
3. Click "Add".
4. Hold the "alt" key and click "More Printers".
5. In the pop up window, select "Advanced" and "Windows Printer with SAMBA", enter the printer name and the printer URI (the format is smb://NAS IP/printer name. The printer name is found on the "Device Configuration" > "USB Printer page"), select "Generic" for Printer Model and click "Add".
6. The printer appears on the printer list and is ready to use.

Note:

- For "Advanced" in Step 5 above, you must hold the "alt" key and click "More Printers" at the same time to view the Advanced printer settings.
- The network printer service of the NAS supports Postscript printer on Mac OS only.

Linux (Ubuntu 10.10)

If you are using Linux (Ubuntu 10.10), follow these steps to configure the NAS printer function:

1. Click the "System" tab, choose "Administration". Then select "Printing".
2. Click "Add".
3. Click "Network Printer", and then select "Internet Printing Protocol (ipp)". Enter the NAS IP address in "Host". "/printers" is already present. Enter the printer name after "printers/" in the field "Queue".
4. Before you continue, click "Verify" to test the printer connection.
5. The operating system starts to search for the possible drivers.
6. Select the printer driver from the built-in database, or search online.
7. Choose the correct printer model and driver. Depending on the printer, some additional printer options may be available in the next step.
8. You can rename this printer or enter additional information. Click "Apply" to exit and finish.
9. The network printer is now available for printing.

UPS

By enabling UPS (Uninterruptible Power Supply) support, you can protect your NAS from abnormal system shutdown caused by power disruption. There are two options provided on the "UPS" page for the NAS during a power failure: 1) turn off the server after the AC power fails, or 2) enter the auto-protection mode after the AC power fails. For option 1, the NAS will shut itself down after the specified time. For option 2, the NAS will stop all running services and unmount all volumes to protect your data after the specified time. For details on NAS behavior during a power failure, refer to the "Behavior of the UPS Feature of the NAS" section. Please note that to protect your data, once the power outage starts, the NAS will automatically turn itself off or enter auto-protection mode (depending on your settings) after 30 seconds regardless of the specified time for either of the above options if the remaining UPS battery charge is < 15%.

In this chapter, the following topics are covered:
- USB Modes
  - Standalone Mode – USB
  - Standalone Mode – SNMP
  - Network Master Mode
  - Network Slave Mode
- Behavior of the UPS Feature of the NAS

USB Modes

Standalone Mode – USB
To operate under USB standalone mode, follow the steps below:
1. Plug in the USB cable on the UPS to the NAS.
2. Choose between whether the NAS will shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
3. Click "Apply All" to confirm.

Standalone Mode – SNMP
To operate under SNMP standalone mode, follow the steps below:
1. Make sure the NAS is connected to the same physical network as the SNMP-based UPS.
2. Enter the IP address of the SNMP-based UPS.

154

3. Choose between whether the NAS should shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Click "Apply All" to confirm.

Network Master Mode

A network UPS master is responsible for communicating with network UPS slaves on the same physical network regarding critical power status. To set your NAS with UPS as network master mode, plug in the USB cable on the UPS to the NAS and follow these steps:

1. Make sure the NAS (the "UPS master") is connected to the same physical network as the network UPS slaves.
2. Click "Enable network UPS Support". This option only appears when your NAS is connected to the UPS by a USB cable.
3. Choose between whether the NAS should shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Enter the "IP address" of other network UPS slaves to be notified in the event of power failure.
5. Click "Apply All" to confirm and continue the setup for the NAS systems which operate in network slave mode below.

Network Slave Mode

A network UPS slave communicates with network UPS master to receive the UPS status. To set up your NAS with UPS as network slave mode, follow these steps:

1. Make sure the NAS is connected to the same physical network as the network UPS master.
2. Select "Network UPS slave" from the "Protocol" drop down menu.
3. Enter the IP address of the network UPS server.
4. Choose between whether the NAS should shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
5. Click "Apply All" to confirm.

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

Behavior of the UPS Feature of the NAS

There are three phases during a power outage:
- Phase 1: Power loss starts until the end of the waiting time.
- Phase 2: From the end of the waiting time to the point when the UPS device runs out of its battery.
- Phase 3: After the UPS device runs out of its battery and until the power restores.

Phase 1:
As soon as the power loss starts, the NAS will detect the UPS device's battery. If the remaining UPS battery charge is < 15%, the system will automatically turn itself off or enter auto-protection mode (depending on your settings) after 30 seconds regardless the time you specified for either of the settings (turn off the NAS or enter auto protection mode.) If the UPS battery charge is > 15%, the NAS will wait for the specified time you entered in the "UPS" page.

If the power resumes during this phase, the NAS will remain in operation.

Phase 2:
Depending on your setting on the "UPS" page:
- If in auto-protection mode, the NAS will stop all running services and unmount all volumes. The NAS at this moment will become inaccessible.
- If the NAS is powered off, it will remain off.

If the power resumes during this phase:
- If in auto-protection mode, the NAS will reboot and resume its previous state.
- If the NAS is powered off, it will remain off.

Phase 3:
Depending on your setting on the "UPS" page:
- If in auto-protection mode, the NAS will lose its power and shut down.
- If the NAS is powered off, it will remain off.

After the power resumes during this phase, the NAS will react according to your settings in "System Settings" > "Power Recovery".

System Status

Go to "Control Panel" > "System Settings" > "System Status" to check the status of your NAS.

System Information

View the summary of system information such as the server name, CPU, memory, firmware and system up time on this page.

> **Note:** CPU and memory information is only available on certain NAS models.

Network Status

View the current network settings and statistics on this page. They are displayed based on network interface. Click the up arrow in the top right to collapse the interface page and the down arrow to expand it.

System Service

View the current settings of system services provided by the NAS.

Hardware Information

View basic hardware information of the NAS.

System Logs

Go to "Control Panel" > "System Settings" > "System Logs" to configure the logs settings of your NAS.

System Event Logs

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

> **Tip:** Right click on a record to delete it. To clear every log, click "Clear All".

System Connection Logs

The NAS can create logs whenever users access, create, delete, move, or rename files and folders using the following protocols:

- AFP (Mac)
- FTP
- HTTP/HTTPS
- iSCSI
- RADIUS
- SMB (Windows)
- SSH
- Telnet

- VPN

Note: For AFP and SSH connections, the system can only record login and logout events.
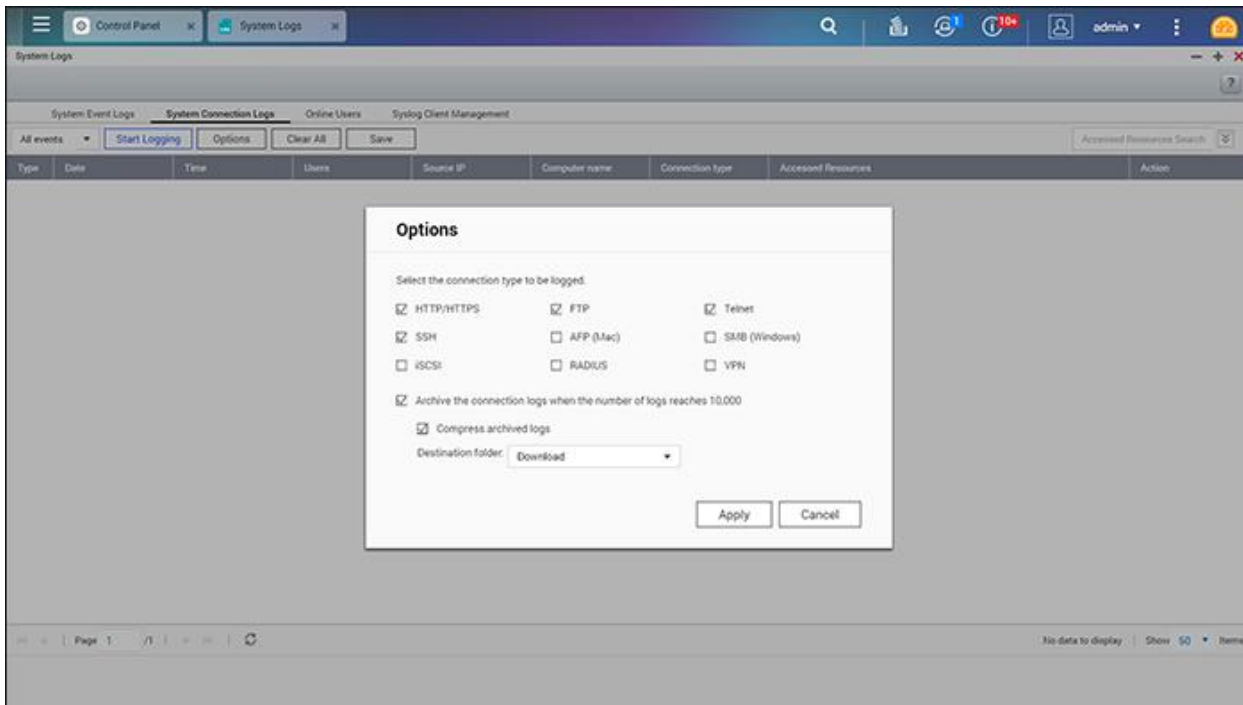
You can perform the following actions on this screen:

Action	Description
Start or stop recording events	Click "Start Logging" or "Stop Logging".
Configure settings	1. Click "Options" and configure the following settings: • Select the protocols to be monitored. • Select "Archive the connection logs when the number of logs reaches 10,000". **Note:** QTS automatically exports the logs (including file-level access lo when the number of logs reaches the limit. 2. You can also perform the following actions: • Select "Compress archived logs". • Specify the folder where the CSV file is to be exported.
Add IP addresses to the block list	Right-click a log entry, select "Add to the block list", and specify the blocking duration.

Delete individual log entries	Right-click a log entry and select "Delete this record".
Delete all log entries	Click "Clear All".

Warning: File transfer performance may be slightly impacted when this feature is enabled.

Online Users

The information of online users connected to the NAS by networking services is shown here.

> **Tip:** Right click on a record to disconnect the IP connection and block the IP.

Syslog Client Management

Syslog is a standard for forwarding log messages on an IP network. Enable this option to save event and connection logs to a remote Syslog server. When converting connection logs into a CSV file, the connection type and action will be number coded. Refer to the table for code meanings.

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

Advanced Log Search

Advanced log search is provided to search for system event logs, system connection logs and online users based on user preferences. First, specify the log type, users, computer name, date range and source IP and click "Search" to search for desired logs or reset to list all logs. Please note that for online users, only the source IP and Computer name can be specified.

Resource Monitor

You can view the CPU usage, disk usage, and bandwidth transfer statistics of the NAS by going to "Main Menu" > "Resource Monitor" to open the Resource Monitor window.
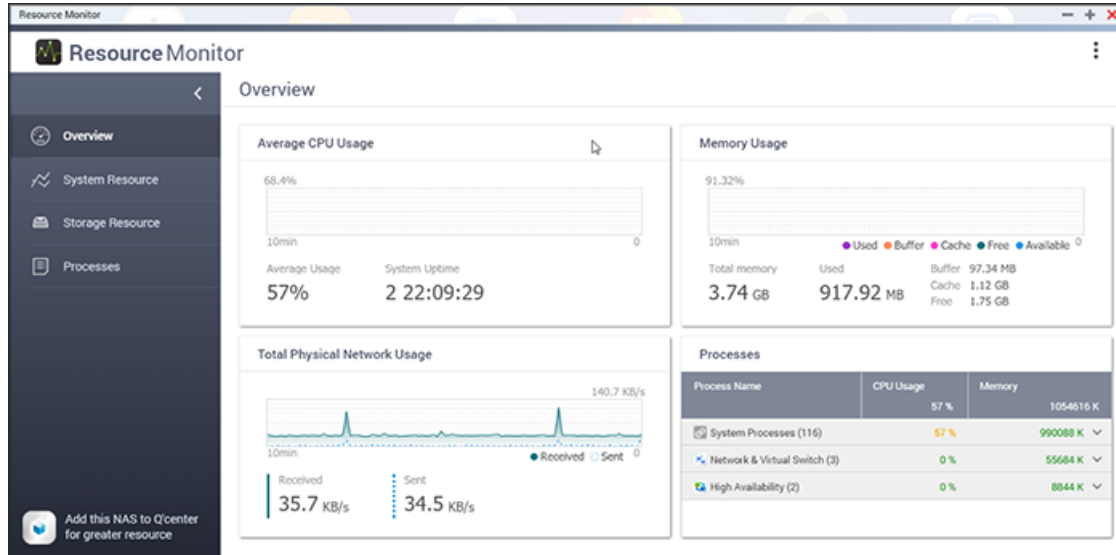
> **Note:** On some models, resource monitor is not available in the Main Menu. On those models, go to "Control Panel" > "Overview" > "System Status" > "Resource Monitor".

Below are the sections of the Resource Monitor (Main Menu version).
- Overview: Displays CPU usage, memory usage, network usage, and system processes.
- System Resource:
  - o CPU: Displays detailed information about CPU usage.
  - o Memory: Displays detailed information about memory usage.
  - o Network: Displays detailed information about network usage.
- Storage Resource:
  - o Volume/LUN Activity: Displays activity on volume/LUN.
  - o RAID Activity: Displays activity of RAID groups.
  - o Disk Activity: Dispalys activity of disks.
  - o Storage Space: Displays the disk space usage of each disk volume and its shared folders.
- Processes: Shows information about the processes running on the NAS.

Below are the sections of the Resource Monitor (System Status version).
- CPU Usage: Shows the CPU usage of the NAS.
- Memory Usage: Shows the memory usage of the NAS by real-time dynamic graph.
- Disk Usage: Shows the disk space usage of each disk volume and its shared folders.

- Bandwidth Usage: Provides bandwidth transfer information of each available NAS LAN port.
- Process: Shows information about the processes running on the NAS.
- Disk Performance: Shows IOPS and latency of the selected volume.

Privilege Settings

Go to "Control Panel" > "Privilege Systems" to configure privilege settings, disk quotas and domain security on the NAS.
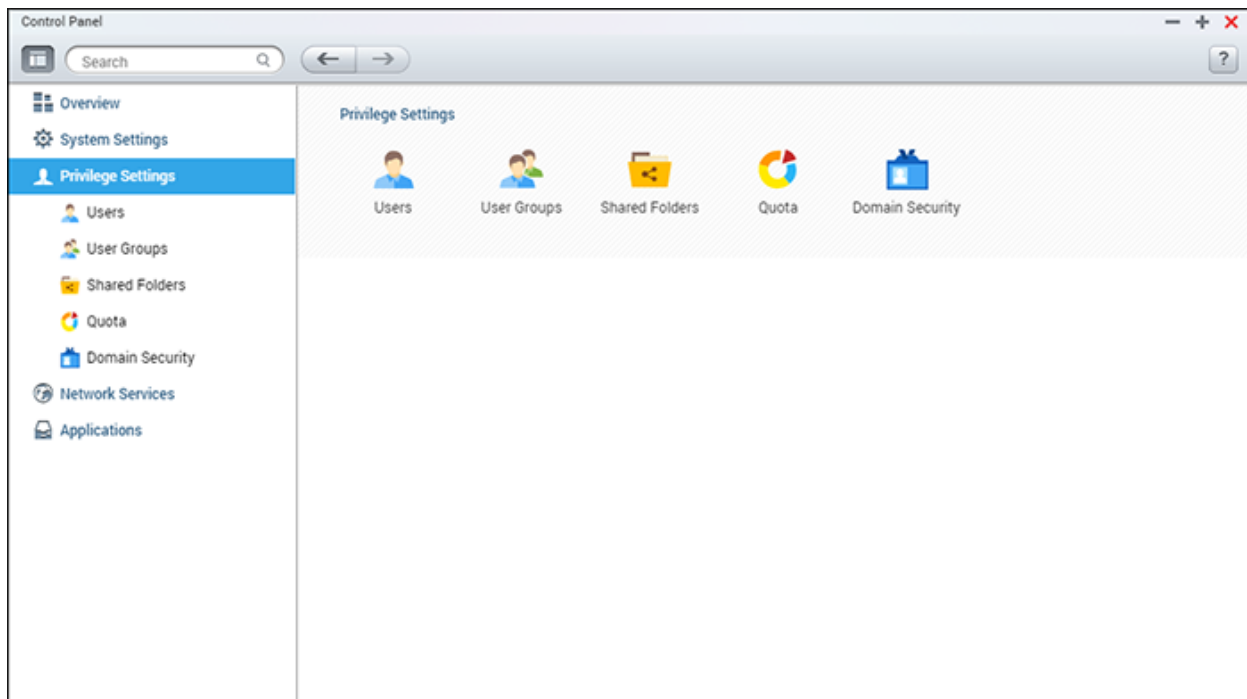
For setup details, refer to the following links:
* Users
* User Groups
* Share Folders
* Quota
* Domain Security

Users

The NAS creates the following users by default:

- admin: Has full access to system administration screens and all shared folders. You cannot delete this user.
- guest: Does not belong to any user group and is not displayed on the "User Management" screen

> **Note:** The login password is "guest".

- anonymous: Is not displayed on the "User Management" screen. You can use this user when connecting to a NAS by FTP.

You can create users based on where the account information is stored.

- Domain user: User name and password are stored on a domain controller
- Local user: User name and password are stored on the NAS

> **Note:** You can edit the account profile, user group, shared folder permissions, and application privileges for users of both types.
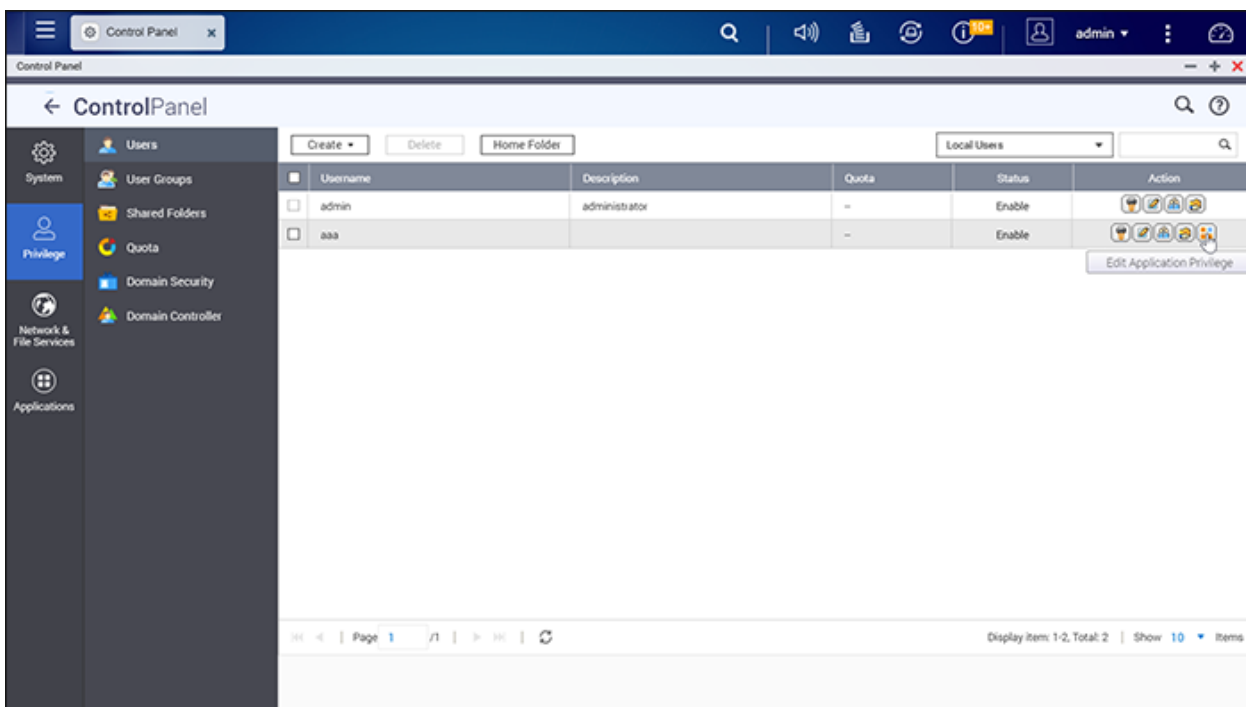
The number of users you can create on the NAS varies by NAS models. If your NAS models are not listed, visit http://www.qnap.com for more details.

Maximum number of users	NAS models
1,024	TS-110, TS-210
2,048	TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
4,096	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP, TS-269 Pro, TS-269L, TS-469 Pro, TS-469L, TS-569 Pro, TS-569L, TS-669 Pro, TS-669L, TS-869 Pro, TS-869L, TS-251, TS-451, TS-651, TS-851, TS-253 Pro, TS-453 Pro, TS-653 Pro, TS-853 Pro, SS-453 Pro, SS-853 Pro.

The following information is required to create new users:

- Username: The username is case-insensitive and supports multi-byte characters, such as Chinese, Japanese, Korean, and Russian. The maximum length is 32 characters. Invalid characters are: " / \ [ ] : ; | = , + * ? < > ` '
- Password: The password is case-sensitive. It is recommended to use a password of at least 6 characters. The maximum length is 64 characters.

In this chapter, the following topics are covered:
- Creating a User
- Creating Multiple Users
- Importing/Exporting Users
- Home Folders

Creating a User

To create a user on the NAS, follow the steps below:
1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Create a User".
3. Follow the wizard instructions to complete the details.

Creating Multiple Users

To create multiple users on the NAS, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Create Multiple Users".
3. Click "Next".
4. Enter the name prefix (for example: "test".) Enter the start number for the username, e.g. 0001 and the number of users to be created (for example: 10.) The NAS will then create ten users named: test0001, test0002, test0003 ... test0010. The password entered here is the same for all the new users.
5. Select to create a private shared folder for each user or not. The shared folder will be named after the username. If a shared folder of the same name has already existed, the NAS will not create the folder.
6. Specify the folder settings.
7. You can view the new users created in the last step. Click "Finish" to exit the wizard.
8. Check that the users have been created.
9. Check that the shared folders have been created for the users.

Importing/Exporting Users

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

Exporting users

Follow the steps below to export users from the NAS:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Import/Export Users".
3. Select the option "Export user and user group settings".
4. Click "Next" to download and save the account setting file (*.bin.) This file can be imported to another NAS for account setup.

Importing users

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

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Import/Export Users".
3. Select "Import user and user group settings". Select the option "Overwrite duplicate users" to overwrite existing users on the NAS. Click "Browse", select the file (*.txt, *.csv, *.bin) which contains the users' information and click "Next" to import the users.
4. Click "Finish" after the users have been created.
5. The imported user accounts will be displayed.

> **Note:**
> - The password rules (if applicable) will not be applied when importing users.
> - The quota settings can be only exported when the quota function is enabled in "Privilege Settings" > "Quota".

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

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 with UTF-8 encoding if it contains double-byte characters.

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

CSV (Excel)

1. Open a new file with Excel.
2. Enter a user's information in the same row in the following order:
   o Column A: Username
   o Column B: Password
   o Column C: Quota (MB)
   o 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 it as a CSV file.
4. Open the CSV file with Notepad and save it in UTF-8 encoding if it contains double-byte characters.

BIN (Exported from the NAS)

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

Home Folders

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

To use this feature, click "Home Folders". Select "Enable home folder for all users" and the disk volume where the home folders will be created in. Click "Apply".

User Groups

A user group is a collection of users with the same access rights to files or folders.

The NAS creates the following user groups by default:

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

The number of user groups you can create on the NAS varies by NAS model. If your NAS is not listed, visit http://www.qnap.com for more details.

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

	Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP, TS-269 Pro, TS-269L, TS-469 Pro, TS-469L, TS-569 Pro, TS-569L, TS-669 Pro, TS-669L, TS-869 Pro, TS-869L, TS-251, TS-451, TS-651, TS-851, TS-253 Pro, TS-453 Pro, TS-653 Pro, TS-853 Pro, SS-453 Pro, SS-853 Pro.

A group name cannot exceed 256 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones: " / \ [ ] : ; | = , + * ? < > ` '

Creating a User Group

Follow these steps to create a user group on the NAS:
1. Go to "Control Panel" > "Privilege Settings" > "User Groups".
2. Click "Create", enter the group name and description, assign users to the group, and edit shared folder permissions (Read Only, Read/Write, and Deny) for the group.
3. Click "Create".

Deleting a User Group

Follow these steps to delete a user group on the NAS:
1. Go to "Control Panel" > "Privilege Settings" > "User Groups".
2. Select the user group(s) to be deleted.
3. Click "Delete".

Tip: You can use the buttons under "Action" to view group details, edit group users, or edit shared folder permissions for a particular user group.

Shared Folders

Go to "Control Panel" > "Privilege Settings" > "Shared Folders" to configure shared folders of your NAS.

This chapter covers the following topics:

- Shared Folders
- Folder Encryption
- ISO Shared Folders
- Folder Aggregation

Shared Folders

You can create multiple shared folders on the NAS and specify the access rights of the users and user groups to the shares. The number of shared folders you can create on the NAS varies according to the NAS models. If your NAS model is not listed, please visit http://www.qnap.com for details.

Maximum number of shared folders	NAS models
256	TS-110, TS-210, TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-x20, TS-x21, TS-410, TS-239 Pro II+, TS-259

	Pro+
512	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-x70, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP, TVS-471, TVS-671, TVS-871, TVS-871U-RP, TVS-1271U-RP, TVS-463, TVS-663, TVS-863, TVS-863+.

To create a shared folder, follow the steps below:

1. Click "Create" > "Shared Folder".
2. Enter the basic folder settings.
   - Folder name: Enter the share name. The share name does not support " / \ [ ] : ; | = , + * ? < > ` '
   - Comment: Enter an optional description of the shared folder.
   - Disk Volume: Select which disk volume on which to create the folder.
   - Path: Specify the path of the shared folder or select to let the NAS specify the path automatically.
3. Access privileges for users: Select the way you want to specify access rights to the folder. If you select to specify the access rights by user or user group, you can select to grant read only, read/write, or deny access to the users or user groups.
4. Folder Encryption: Select to enable folder encryption with 256-bit AES encryption. See [Folder Encryption](#) for more information.
5. Advanced settings (this is only available when creating a shared folder)
   - Guest Access Right: Assign guest access rights of the folder.
   - Media Folder: Set the shared folder as a media folder.
   - Hidden Folder Hide Network drive: Hide the shared folder or not in Microsoft Networking. When a shared folder is hidden, you have to enter the complete directory \\NAS_IP\share_name to access the share.
   - Lock File (Oplocks): Opportunistic locking is a Windows mechanism for the client to place an opportunistic lock (oplock) on a file residing on a server in order to cache the data locally for improved performance. Oplocks is enabled by default for everyday usage and should be disabled on networks that require multiple users concurrently accessing the same files.
   - SMB Encryption: Set the folder to be accessible for SMB 3 clients. This option is only available after SMB3 is enabled. After this opton is enabled, all communications via

Microsoft Networking will be conducted via SMB3 and encrypted. All SMB3 clients will be able to connect to NAS via Microsoft Networking.

- o Recycle Bin: Enable the Network Recycle Bin for created shared folders. "Restrict the access of Recycle Bin to administrators only for now" will ensure that files deleted and moved to the Network Recycle Bin can only be recovered by administrators. Please note that the Recycle Bin option is only available after you enable Network Recycle Bin in "Control Panel" > "Network Services" > "Network Recycle Bin".
- o Enable Sync on this shared folder: Enable this option if you want to sync the content in this shared folder. Refer to [Qsync Central Station](#) for more details.
6. Click "create" to complete the setup.

To delete a shared folder, select the folder checkbox and click "Remove". You can select the option "Also delete the data. (Mounted ISO image files will not be deleted)" in the dialog box to delete the folder and the files it contains. If you do not choose to delete the folder data, the data will be retained on the NAS. You can create a shared folder of the same name again to access the data.

Icon	Name	Description
✏️	Folder Property	Edit the folder property. Specify folder name, comment, disk volume, path and decide whether to hide or show the network drive, enable oplocks, restrict the access of Recycle Bin to administrators (files can only be recovered by administrators from the Network Recycle Bin) ,enable write-only access on FTP connection, folder encryption, and synchronization.
🗂️	Folder Permissions	Edit folder permissions and subfolder permissions.
🔄	Refresh	Refresh the shared folder details.

Tip: In the event that default shared folders are removed due to human errors (such as accidental hard drive removal), you can try to restore them by clicking "Restore Default Shared Folders" after the errors are fixed.

Folder Permissions
Configure folder and subfolder permissions on the NAS. To edit basic folder permissions, locate a folder in "Privilege Settings" > "Shared Folders" and click "Folder Permissions". Folders are shown on the left panel and the users with permission to access these folders are shown on the right panel. You can also specify guest privileges on the bottom panel. Click "Add" to select more users and user groups, specify their privileges for the folder, and click

"Add" to confirm. Click "Remove" to remove any configured permissions. You can select multiple items by holding the Ctrl key and left clicking them.

Subfolder Permissions

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

To configure subfolder permissions, follow the steps below:

1. Go to "Privilege Settings" > "Shared Folders" > "Advanced Permissions" tab. Select "Enable Advanced Folder Permissions" and click "Apply".
2. Go to "Privilege Settings" > "Shared Folders" > "Shared Folder" tab. Select a root folder and click "Folder Permissions". The shared folder name and its first-level subfolders are shown on the left. Users with permission to access the folder are shown in the panel, with special permission below. Double click the first-level subfolders to view the second-level subfolders. Select the root folder and click "Add" to specify read only, read/write, or deny access for users and user groups.
3. Click "Add" when you finish configuring settings.
4. Specify other permissions settings below the folder permissions panel.
   o Guest Access Right: Specify whether to grant full or read only access or deny guest access.
   o Owner: Specify the owner of the folder. By default, the folder owner is the creator.
5. To change the folder owner, click the "Folder Property" button next to the owner field.
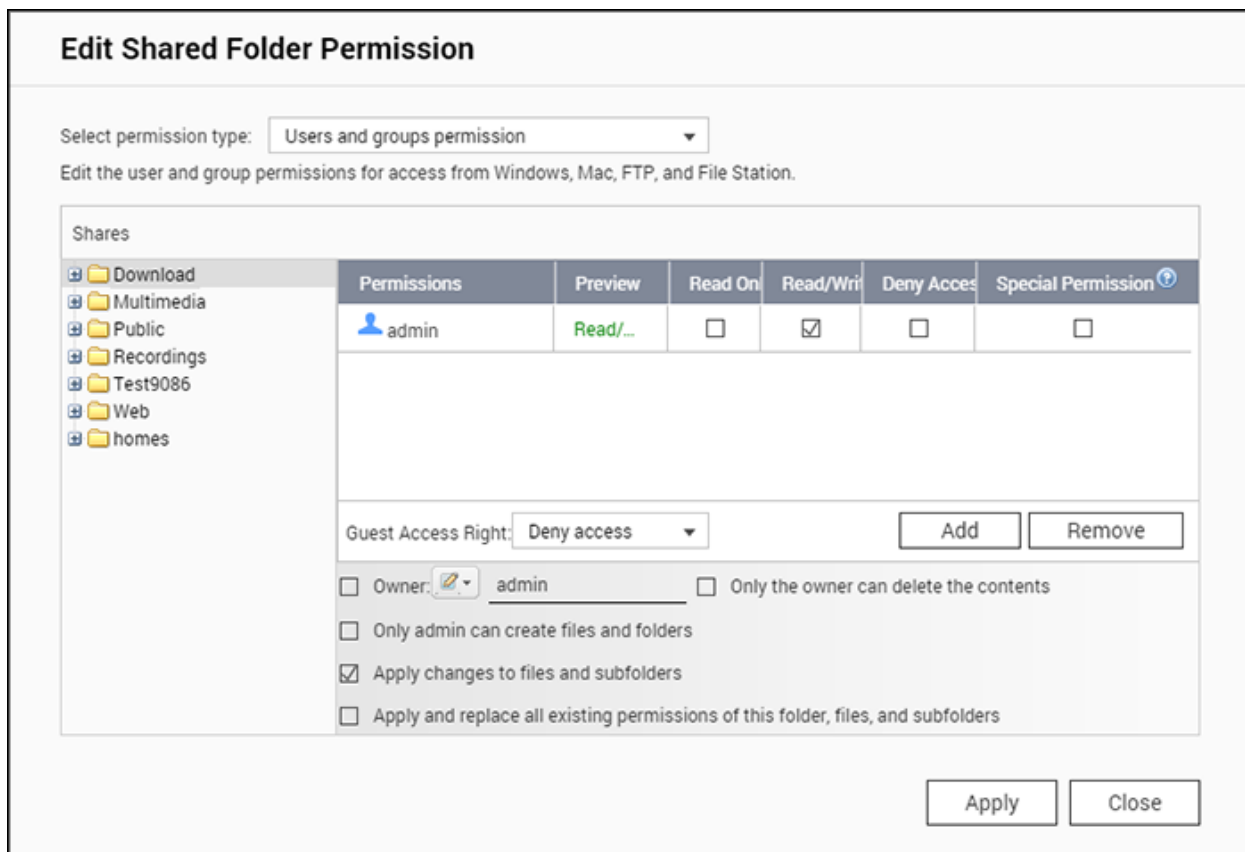
6. Select a user from the list or search for a username and then click "Set".
   - Only the owner can delete the contents: When you apply this option to a folder, only the folder owner can delete the first-level subfolders and files. This option does not apply to the subfolders of the selected folder even if the options "Apply changes to files and subfolders" and "Apply and replace all existing permissions of this folder, files, and subfolders" are selected.
   - Only admin can create files and folders: This option is only available for root folders. Select this option to allow admin to create first-level subfolders and files in the selected folder only. Other users with read/write access to the root folder can only create files and folders in the second and lower-level subfolders.
   - Apply changes to files and subfolders: Apply permissions settings except owner protection and root folder write protection to all the files and subfolders in the selected folder. These settings include new users, deleted users, modified permissions, and folder owner. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.
   - Apply and replace all existing permissions of this folder, files, and subfolders: Select this option to override all previously configured permissions of the selected folder and its files and subfolders except owner protection and root folder write protection. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.
   - Special Permission: This option is only available for root folders. Select this option and choose between "Read only" or "Read/Write" to allow a user to access to all the content of a folder regardless of the pre-configured permissions. A user with special permission will be identified as "admin" when he/she access the folder via Microsoft Networking. If you have granted "Read/Write" permission to the user, this user will have full access and is able to configure the folder permissions on Windows. Please note that all the files created by this user belong to "admin". Because "admin" does not have quota limit on the NAS, the number and size of the files created by users with special permission will not be limited by their pre-configured quota settings. This option should be used for administrative and backup tasks only.
7. After changing the permissions, click "Apply" and then "YES" to confirm.

Note:
- You can create up to 230 permission entries for each folder when Advanced Folder Permission is enabled.
- If you specify "deny access" for a user on the root folder, the user will not be allowed to access the folder and subfolders even if you select read/write access to the subfolders.

- If you specify "read-only access" for a user on the root folder, the user will have read only access to all the subfolders even if you select read/write access to the subfolders.
- To specify read-only permission on the root folder and read/write permission on the subfolders, you must set read/write permission on the root folder and use the option "Only admin can create files and folders" (to be explained later).
- If an unidentified account ID is shown for a subfolder on the permission assignment page after you click "Access Permissions" next to a shared folder in "Control Panel">"Privilege Settings">"Shared Folders">"Shared Folder", it is likely that the permission of that subfolder has been granted to a user account that no longer exists. In this case, please select this unidentified account ID and click "Remove" to delete it.

Microsoft Networking Host Access Control

NAS folders can be accessed via Samba (Windows) by default. You can specify authorized IP addresses and hosts by following these steps:

1. Click "Folder Permissions".
2. Select "Microsoft Networking host access" from the drop-down menu on top of the page.
3. Specify the IP addresses and host names that are allowed to this shared folder. The following IP address and host name are used as an example:
    o IP address: 192.168.12.12 or 192.168.*.*
    o Host name: dnsname.domain.local or *.domain.local
4. Click "Add" to enter the IP address and host name and then "Apply".

Notifications on characters used:
- Wildcard characters: You can enter wildcard characters in an IP address or host name entry to represent unknown characters.
- Asterisk (*): Use an asterisk (*) as a substitute for zero or more characters. For example, if you enter *.domain.local, the following items are included: a.domain.local, cde.domain.local, or test.domain.local
- Question mark (?): Use a question mark (?) as a substitute for only one character. For example, test?.domain.local includes the following: test1.domain.local, test2.domain.local, or testa.domain.local

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

Folder Encryption

Shared folders on the NAS can be encrypted with 256-bit AES encryption to protect data. The encrypted shared folders can only be mounted for normal read/write access with the

authorized password. The encryption feature protects the confidential data in the folder from unauthorized access even if the hard drives or the entire NAS were stolen.

> **Note:**
> - The function or its content is only applicable on some models.
> - The encryption key cannot include dollar signs ($) or equal signs (=).
> - Encrypted shared folders cannot be accessed via NFS.
> - If a volume has been encrypted, the shared folders on that volume cannot be encrypted.
> - Only x86 models support folder encryption.
> - Only x86 models or ARM models that have been updated to firmware 4.1.1 or newer support volume encryption.

Encrypting and locking a shared folder

To encrypt and lock a shared folder, follow these steps:

1. Enable folder encryption:
   - When you create a folder, click "Encryption" under "Folder Encryption", enter a password and choose to save an encryption key.
   - To encrypt an existing folder, click "Edit Properties" under "Action" in "Control Panel" > "Privilege Settings" > "Shared Folders", click "Encrypt this folder", enter a password and choose to save encryption key.
2. Go to "Control Panel" > "Privilege Settings" > "Shared Folders", click "Encryption Management" under "Action".
3. Switch to "Lock" and click "OK".

Encryption verification

After a folder is locked, that folder will be invisible in File Station.   If an encrypted shared folder is unlocked, it will reappear in File Station.

Unlocking a shared folder

To unlock an encrypted and locked shared folder, go to "Control Panel" > "Privilege Settings" > "Shared Folders", click "Encryption Management" under "Action" and enter the password or upload the encryption key file.

Encryption Management

After the folder is encrypted, click "Encryption Management" under "Action" in "Control Panel" > "Privilege Settings" > "Shared Folders" to edit encryption settings:
- To save the encryption key, select the "Download" tab and enter the encryption password to export the key.

- You can choose to automatically mount the encrypted folder by selecting "Mount automatically on start up" in the "Save" tab. Enter the encryption key to mount the folder automatically for access. This option will be automatically enabled if the "Save encryption key" is checked when encrypting the folder. Folders that do not have this option enabled will be locked after the system restarts.
- To prevent access to the encrypted folder, enable the lock function in the "Lock" tab. Select "Forget the saved key" if you want the folder to remain locked after the system restarts (i.e., without auto mount when system starts.) To unlock the folder later, click "Unlock Share Folder" and then enter or import the encryption key to unlock the folder.

> **Note:**
> - It is strongly recommended that you export and save the encryption key. You need the key to unlock or decrypt the encrypted folder.
> - You cannot change an encrypted folder's volume or path.
> - NAS also offers volume-based encryption. See [Volume Encryption](#) for more details.
> - The default shared folders cannot be encrypted.

ISO Shared Folders

You can mount ISO image files on the NAS as ISO shares. The NAS supports mounting up to 256 ISO shares.

TS-110, TS-119, TS-120, TS-121, TS-210, TS-219, TS-219P, TS-220, TS-221, TS-410, , TS-119P+, TS-219P+, TS-112, TS-212 support up to 256 network shares only (including 6 default network shares). The maximum number of ISO image files supported by these models is less than 256 (256 minus 6 default shares minus number of network recycle bin folders).

Follow these steps to mount an ISO file on the NAS using the web interface:
1. Log in to the NAS as an administrator. Go to "Share Folders" > "Create". Click "Create an ISO Share".
2. Select an ISO image file on the NAS. Click "Next".
3. The image file will be mounted as a shared folder of the NAS. Enter the folder name.
4. Specify the access rights of NAS users or user groups to the shared folder. You can also select "Deny Access" or "Read only" for the guest access right. Click "Next".
5. Confirm the settings and click "Next".
6. Click "Finish".
7. After mounting the image file, you can specify access rights for users over different network protocols such as SMB, AFP, NFS, and WebDAV by clicking the Access Permission icon in the "Action" column.

The NAS supports mounting ISO image files using File Station. Refer to the [File Station](#) chapter for more details.

> **Note:**
> - ARM-based NAS models do not support using Cyrillic characters for the name of a subfolder in an ISO shared folder (the name will be incorrectly displayed if a subfolder is created with a Cyrillic name.) Please name the subfolder with a different language before an ISO file is created.
> - For Mac OSX, mounting a folder that contains the # character in the folder name through WebDAV is not supported. Please rename the folder before mounting it if necessary.

Folder Aggregation

You can aggregate the shared folders on Microsoft network as a portal folder on the NAS and let NAS users access the folders through your NAS. Up to 10 folders can be linked to a portal folder. To use this function, follow these steps:

1. Enable folder aggregation.
2. Click "Create a Portal Folder".
3. Enter the portal folder name. Decide whether to hide the folder, and enter an optional comment for the portal folder. Select the option "User must login before accessing the portal folder" to avoid guest access and permission issues on the shared folders.
4. Click the "Link Configuration" button under "Action" and enter the remote folder settings. Make sure the folders are open for public access.
5. Upon successful connection, you can connect to the remote folders through the NAS.

> **Note:**
> - Folder Aggregation is only supported in Microsoft networking service and is recommended for a Windows AD environment.
> - If there is permission control on the folders, you need to join the NAS and the remote servers to the same AD domain.

Advanced Permissions

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

Protocols	Permission	Options	How to Configure
Advanced Folder Permissions	FTP, AFP, File Station, Samba	3 (Read, Read & Write, Deny)	NAS web UI

| Windows ACL | Samba | 13 (NTFS permissions) | Windows File Explorer |
| Both | FTP, AFP, File Station, Samba | Please see the application note (https://www.qnap.com/i/en/trade_tea ch/con_show.php?op=showone&cid=6) for more details. | Windows File Explorer |

Advanced Folder Permissions

Use "Advanced Folder Permissions" to directly configure subfolder permissions on the NAS. There is no depth limitation for subfolder permission, but it is highly recommended to only change permissions on the first or second subfolder level. When "Advanced Folder Permissions" is enabled, click "Folder Permissions" under the "Shared Folders" tab to configure subfolder permission settings. See Shared Folders" > "Folder Permission" for more information.

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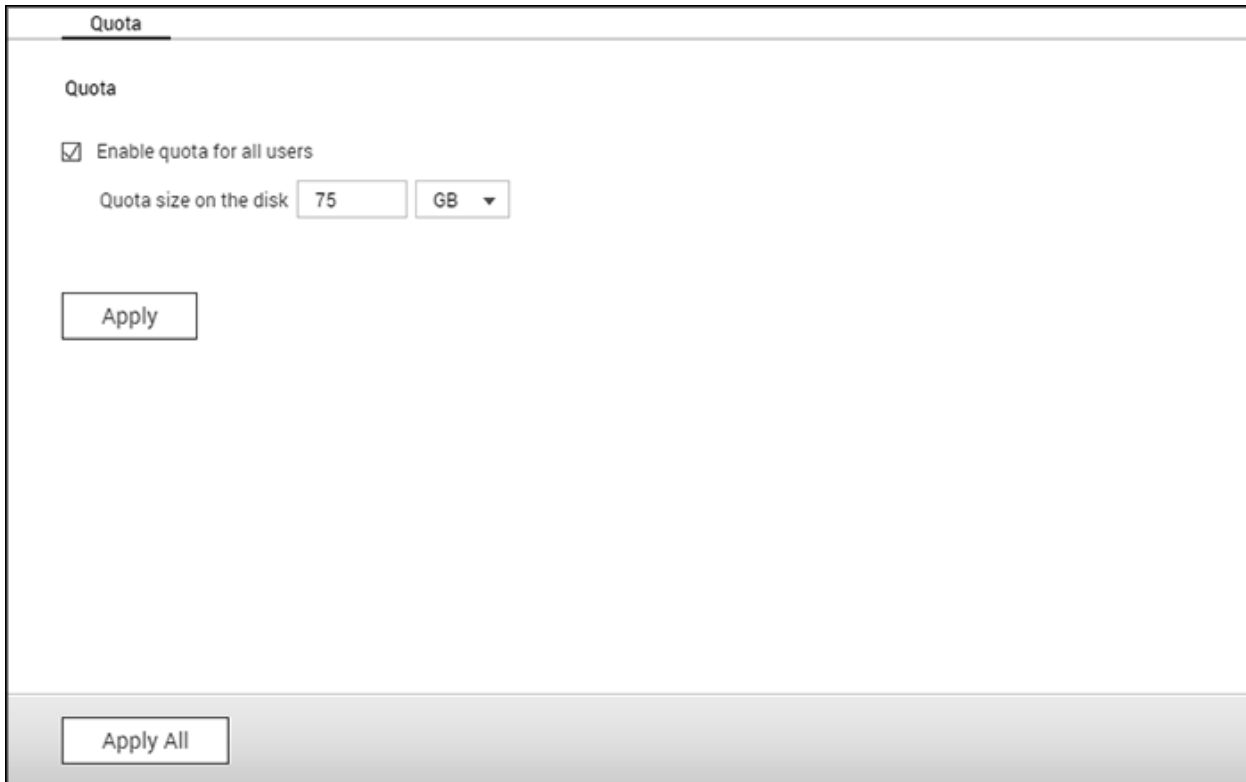
Use "Windows ACL" to configure the subfolder and file level permissions from Windows File Explorer. All Windows Permissions are supported. For detailed Windows ACL behavior, please refer to standard NTFS permissions: http://www.ntfs.com/ntfs-permissions.htm

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

Note: Only the "List Folders" / "Read Data" and "Create Files" / "Write Data" permissions will be available when you use other file protocols (such as AFP, NFS, FTP, WebDAV, etc)

Quota

To efficiently allocate storage space, you can specify a quota value (in megabytes or gigabytes) that applies to all users and disk volumes. QTS prevents users from uploading data to the NAS when the feature is enabled and the quota is reached.
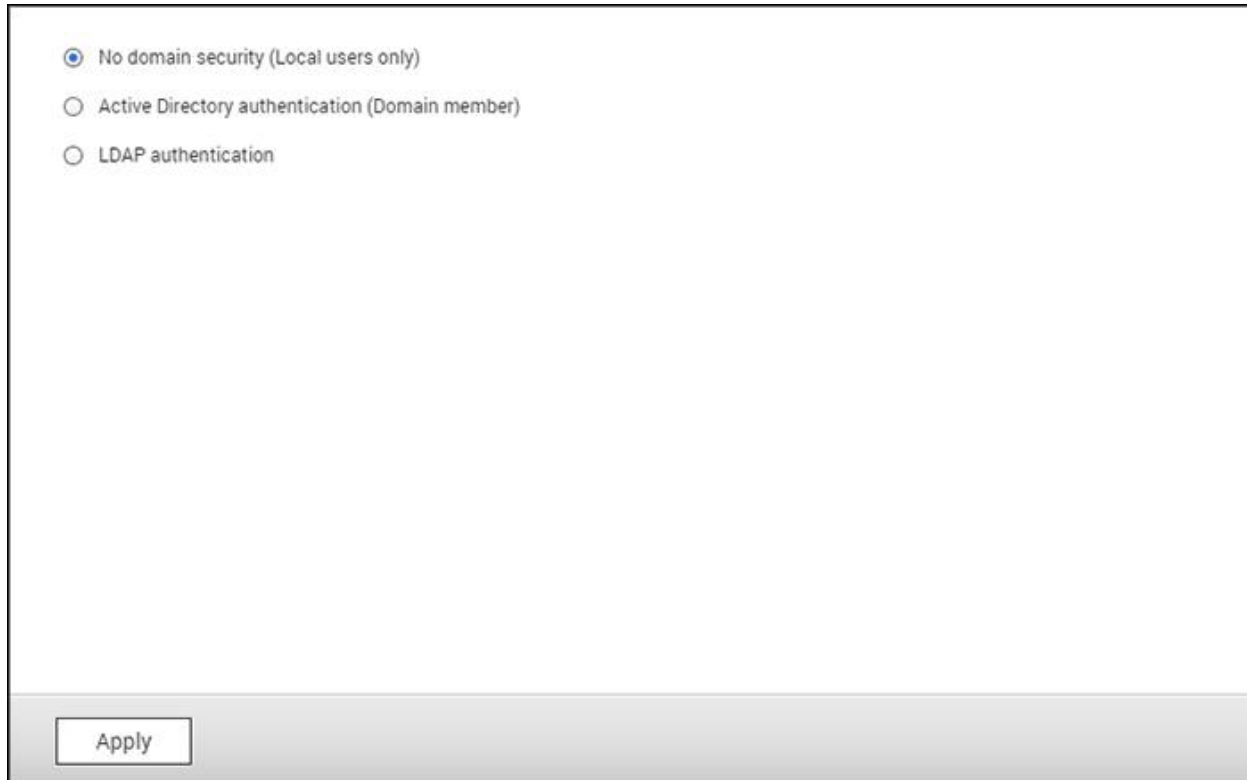
After the quota is specified and applied, the screen displays a list of all local and domain users and the corresponding storage details (quota size, used space, and available space). You can perform the following actions:

- Modify quota settings: Click "Edit" and then specify a new quota value or select "No limit".
- Export quota settings to a CSV file: Click "Generate".
- Download generated CSV files: Click "Download" and then save the file to a preferred location.

Domain Security

The NAS supports user authentication by local access right management, Microsoft Active Directory (Windows Server 2008/2012), and Lightweight Directory Access Protocol (LDAP) directory.

By joining the NAS to an Active Directory or a LDAP directory, the AD or LDAP users can access the NAS using their own accounts without extra user account setup on the NAS.

*   **No domain security:** Only the local users can access the NAS.
*   **Active Directory authentication (domain members):** Join the NAS to an Active Directory. The domain users can be authenticated by the NAS. After joining the NAS to an AD domain, both the local NAS users and AD users can access the NAS via the following protocols/services:
    *   Samba (Microsoft Networking)
    *   AFP
    *   FTP
    *   File Station
*   **LDAP authentication:** Connect the NAS to an LDAP directory. The LDAP users can be authenticated by the NAS. After connecting the NAS to an LDAP directory, either the local NAS users or the LDAP users can be authenticated to access the NAS via Samba (Microsoft Networking). Both the local NAS users and LDAP users can access the NAS via the following protocols/services:
    *   AFP
    *   FTP
    *   File Station

Joining NAS to Active Directory (Windows Server 2003/2008/2012)

Active Directory is a directory used in Windows environments to centrally store, share, and manage a network's information and resources. It is a hierarchical data center which centrally holds information for 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 automatically imported to the NAS. AD users can use their same login details to access the NAS. If you are using Active Directory with Windows Server 2008 R2, you must update the NAS firmware to at least 3.2.0 to join the NAS to the AD.

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

To join the NAS to an AD domain by the Quick Configuration Wizard, follow these steps:
 1. Login to the NAS as an administrator. Go to "Privilege Settings" > "Domain Security". Select "Active Directory authentication (domain member)" and click "Quick Configuration Wizard".
 2. Read the wizard introduction. Click "Next".
 3. Enter the full domain name of the AD domain (DNS.) The NetBIOS name will be automatically generated from the domain name but can be changed manually if the name is different than the generated one. Specify the DNS server IP for domain resolution. The IP must be the same as the DNS server of your Active Directory. Click "Next".
 4. Select the domain controller from the multiple selection window. For domain controller redundancy, select multiple domain controllers and set the order of priority for the controllers. The domain controller is responsible for time synchronization between the NAS and the domain server and user authentication. Enter the domain administrator name and password. Click "Join".
 5. Upon successful login to the domain server, the NAS has joined to the domain. Click "Finish" to exit the wizard.
 6. Go to "Privilege Settings" > "Users" or "User Groups" to load the domain users or user groups to the NAS.

Joining the NAS to Active Directory (AD) by Quick Configuration Manually

Follow the steps below to join the QNAP NAS to the Windows Active Directory.
 1. Login to the NAS as an administrator. Go to "Control Panel" > "System" > "General Settings" > "Time". Set the date and time of the NAS to synchronize with you domain

controller time as it must be consistent with the time of the AD server. The maximum time disparity tolerated is 5 minutes.

2. Go to "Control Panel" > "Network & File Services". Click" Network & Virtual Switch" and go to "Interfaces". Click "DNS Server" and set the IP of the primary DNS server as the IP of the Active Directory server that contains the DNS service. The primary DNS server field must be the IP of the DNS server that is used for your Active Directory. If you use an external DNS server, you will not be able to join the domain.

3. Go to "Control Panel" > "Privilege" > "Domain Security". Select "Active Directory authentication (domain member)", click "Manual Configuration".

4. Enter the AD domain information, click "Join".

Note:

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

Windows Server 2008

Check the AD server name and domain name in "Control Panel" > "System" in Windows. In the system dialog window, the AD server name will appear as the computer name and the domain name can be found in the domain field.

Note:

- After joining the NAS to the Active Directory, the local NAS users who have access rights to the AD server should use "NASname\username" to login. AD users should use their own usernames to login to the AD server.
- For TS-x09 series NAS, if the AD domain is based on Windows 2008 Server, the NAS firmware must be at least version 2.1.2.

Windows 7

If you are using a Windows 7 PC that 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:

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

2. Click "Local Security Policy".

3. Go to "Local Policies" > "Security Options". Select "Network security: LAN Manager authentication level".

4. In "Local Security Setting" select "Send LM & NTLMv2 – use NTLMv2 session security if negotiated" from the list. Then click "OK".

Verifying the settings

To verify that the NAS has successfully joined the Active Directory, go to "Privilege Settings" > "Users" and "User Groups". A list of users and user groups will be shown on the "Domain Users" and "Domain Groups" lists respectively. If you have created new users or user groups in the domain, you can click the Refresh button to add users and user group lists from the Active Directory to the NAS. The user permission settings will be synchronized in real time with the domain controller.

Connecting NAS to an LDAP Directory

LDAP (Lightweight Directory Access Protocol) is a directory that can store the information of every user and group in a centralized server. Administrators can use LDAP to manage users in the LDAP directory and allow them to connect to multiple NAS with the same login details. This feature is intended for use by administrators and users who have knowledge of Linux servers, LDAP servers, and Samba. A running LDAP server is required when using this feature.

Requirements

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

Connecting QNAP Turbo NAS to LDAP Directory

Follow the steps below to connect the QNAP NAS to an LDAP directory:
1. Login to the NAS as an administrator.
2. Go to "Privilege Settings" > "Domain Security". By default, "No domain security" is enabled. This means only local NAS users can connect to the NAS.
3. Select "LDAP authentication" and complete the settings.
   - LDAP Server Host: The host name or IP address of the LDAP server.
   - LDAP Security: Specify how the NAS will communicate with the LDAP server:
     - ldap:// = Use a standard LDAP connection (default port: 389.)
     - ldap:// (ldap + SSL) = Use an encrypted connection with SSL (default port: 686.) This is normally used by older version of LDAP servers.
     - Ldap:// (ldap + TLS) = Use an encrypted connection with TLS (default port: 389.) This is normally used by newer version of LDAP servers
   - BASE DN: The LDAP domain. For example: dc=mydomain,dc=local
   - Root DN: The LDAP root user. For example cn=admin, dc=mydomain,dc=local
   - Password: The root user password.
   - Users Base DN: The organization unit (OU) where users are stored. For example: ou=people,dc=mydomain,dc=local
   - Groups Base DN: The organization unit (OU) where groups are stored. For example ou=group,dc=mydomain,dc=local

4. Click "Apply" to save the settings. Upon successful configuration, the NAS will be able to connect to the LDAP server.
5. Configure LDAP authentication options.
   o If Microsoft Networking has been enabled (Network Services > Win/Mac/NFS > Microsoft Networking) when applying the LDAP settings, specify the users who can access the NAS via Microsoft Networking (Samba.)
     ▪ Local users only: Only local NAS users can access the NAS via Microsoft Networking.
     ▪ LDAP users only: Only LDAP users can access the NAS via Microsoft Networking.
   o If Microsoft Networking is enabled after the NAS has already been connected to the LDAP server, select the authentication type for Microsoft Networking.
     ▪ Standalone Server: Only local NAS users can access the NAS via Microsoft Networking.
     ▪ LDAP Domain Authentication: Only LDAP users can access the NAS via Microsoft Networking.
6. When the NAS is connected to an LDAP server, the administrator can:
   o Go to "Privilege Settings" > "Users" and select "Domain Users" from the drop-down menu. The LDAP users list will be shown.
   o Go to "Privilege Settings" > "User Groups" and select "Domain Groups" from the drop-down menu. The LDAP groups will be shown.
   o Specify the folder permissions of LDAP domain users or groups in "Privilege Settings" > "Shared Folders" > click the "Access Permissions" button next to the folder to be configured.

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

LDAP Authentication Technical Requirements with Microsoft Networking

Required items to authenticate the LDAP users on Microsoft Networking (Samba):
1. A third-party software to synchronize the password between LDAP and Samba in the LDAP server.
2. Importing the Samba schema to the LDAP directory.

A. Third-party software
Some software applications are available and allow management of LDAP users, including Samba password. For example:
- LDAP Account Manager (LAM), with a web-based interface, available from: http://www.ldap-account-manager.org/
- smbldap-tools (command line tool)

- webmin-ldap-useradmin - LDAP user administration module for Webmin.

B. Samba schema

To import the a Samba schema to the LDAP server, please refer to the documentation or FAQ of the LDAP server. A samba.schema file is required and can be found in the directory examples/LDAP in the Samba source distribution. Example for open-ldap in the Linux server where the LDAP server is running (it can be different depending on the Linux distribution):

Copy the samba schema:

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

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

```
include /etc/ldap/schema/samba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/nis.schema
```

Configuration examples

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

1. Linux OpenLDAP Server
    o Base DN: dc=qnap,dc=com
    o Root DN: cn=admin,dc=qnap,dc=com
    o Users Base DN: ou=people,dc=qnap,dc=com
    o Groups Base DN: ou=group,dc=qnap,dc=com
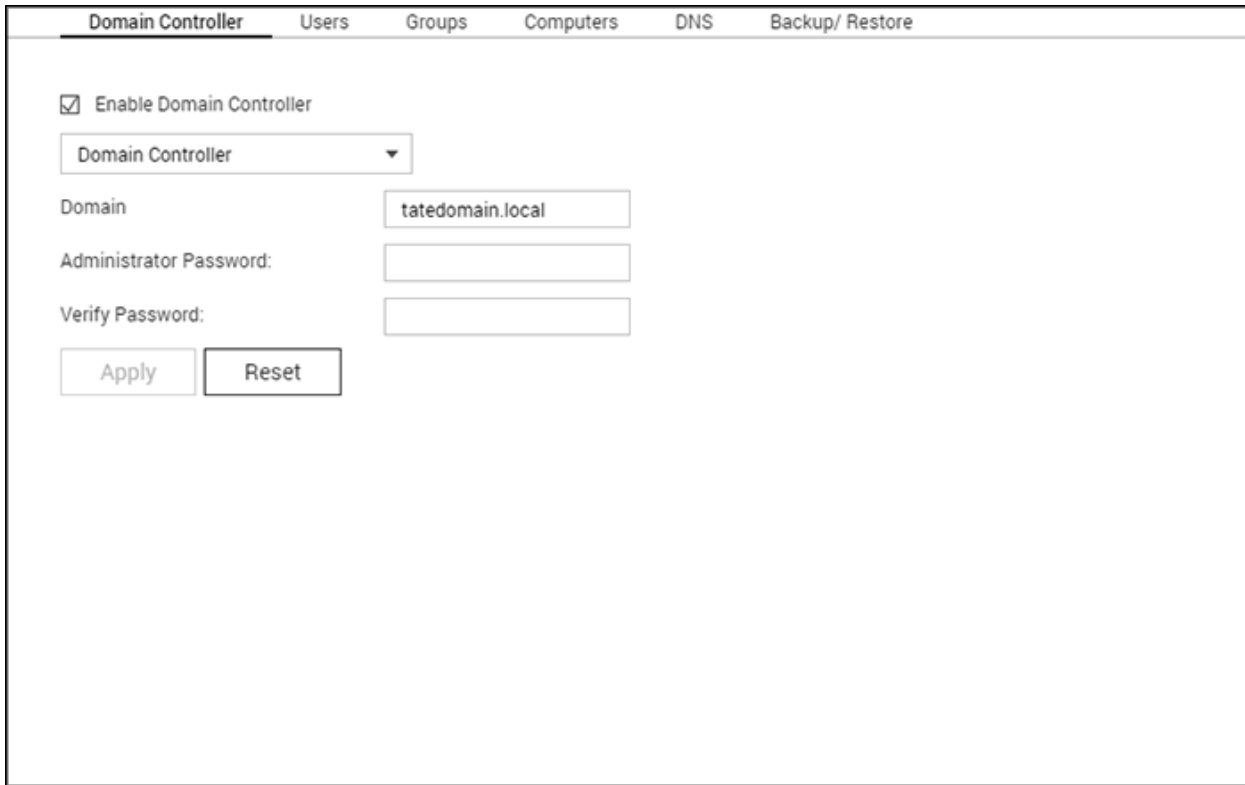
2. Mac Open Directory Server
    o Base DN: dc=macserver,dc=qnap,dc=com
    o Root DN: uid=root,cn=users,dc=macserver,dc=qnap,dc=com
    o Users Base DN: cn=users,dc=macserver,dc=qnap,dc=com
    o Groups Base DN: cn=groups,dc=macserver,dc=qnap,dc=com

Domain Controller

The Turbo NAS can now act as a domain controller for Windows. IT administrators can easily configure the Turbo NAS as the centerpiece of domain directory services for their organization to store user account information, manage user authentication and enforce security for a Windows domain.

| Domain Controller | Users | Groups | Computers | DNS | Backup/ Restore |

☑ Enable Domain Controller

Domain Controller ▼

Domain: tatedomain.local

Administrator Password:

Verify Password:

Apply   Reset

> **Note:** This function is only applicable to some models.

Domain Controller

Three domain controller modes are available for the Turbo NAS:

- Domain Controller: Only a domain controller can create a domain and the first NAS that creates the domain must be a domain controller. In this mode, the NAS can create and authenticate users.
- Additional Domain Controller: In case more than one domain controller is needed, you can choose this mode to add additional domain controllers. The NAS set as an additional domain controller will then act as a domain controller and can create and authenticate users.
- Read-Only Domain Controller: To accelerate the user authentication process on specific sites, it is possible to enable a Read-Only domain controller. Users can be authenticated by this NAS, but it will not be able to create a domain user.

To set the NAS as a domain controller, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Domain Controller" tab.
2. Select a domain controller mode from the drop down list.
3. Specify a domain (example: mydomain.mycompany.local.)
4. Fill out the administrator password and the same password again in the "Verify Password" field.
5. Click "Apply".

After a domain controller is enabled, only the domain users can connect to Microsoft Networking shared folders. Please be sure to grant shared folder permissions to domain users and groups.

> **Note:** The NAS can only act as either a domain controller or LDAP server. If the option "Enable Domain Controller" is grayed out, please disable the LDAP Server in "Control Panel" > "Applications" > "LDAP Server" first.

Users

You can create or delete domain user accounts or manage their membership here.

Creating a user

To create a domain user, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.
2. Click "Create" > "Create a User".
3. Follow the instructions of the wizard to complete the details.

Creating multiple users

To create multiple domain users, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.
2. Click   "Create" > "Create Multiple Users".
3. Click "Next".
4. Enter the name prefix, e.g. test. Enter the start number for the username, e.g. 0001 and the number of users to be created, e.g. 10. The NAS creates ten users named test0001, test0002, test0003…test0010. The password entered here is the same for all the new users.
5. Select to create a private shard folder for each user or not. The shared folder will be named after the username. If a shared folder of the same name has already existed, the NAS will not create the folder.
6. Specify the folder settings.
7. You can view the new users created in the last step. Click "Finish" to exit the wizard.
8. Check that the users have been created.
9. Check that the shared folders have been created for the users.

Batch importing users

To batch import domain users, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.

2. Click   "Create" > "Batch Import Users".

3. Select the option "Overwrite existing users" to overwrite existing domain users (or leave this option unchecked if you want to import domain users without overwriting exist ones.) Click "Browse" and select a CSV file which contains the user information in the following format (account, password, description and email.) For steps to create a CSV file, refer to the next section **Creating a CSV File (Excel)**.

4. Click "Next" to import the users and "Finish" after the users have been created.

5. The imported user accounts will be shown.

> **Note:**
> - The password rules (if applicable) will not be applied when importing the users.
> - The account and password fields can not be empty for an account.

Creating a CSV file (Excel)

1. Open a new file with Excel.

2. Enter an user's information in the same row in the following order:

   o Column A: Account

   o Column B: Password

   o Column C: Description

   o Column D: Email

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.

Deleting users

To delete a domain user account, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users".

2. Select the user account(s) to be deleted.

3. Click "Delete".

4. Click "Yes".

User account management

Refer to the following table for available buttons under "Action" and their explanations:

Button	Name	Description
	Edit Password	Edit the password of a domain user account.
	Edit User Properties	Specify whether the domain user must change the password at the first login, account expiration date, description and email.
	Edit Group Membership	Choose which domain group(s) the domain user belongs to.
	Edit User Profile	Specify the profile path, login script, and home folder of an domain user account.

For user profiles:

- Profile path: Specify the shared folder where the roaming profiles are stored. The path specified can be a shared folder name such as /home or /user1profile, or a UNC path such as \\nas.mydomain.local\home.
- Login script: Specify the logon script to execute when a domain user logs on from a PC member of the domain. Copy the script to the shared folder (sysvol) in the subfolder {your_domain}\scripts by connecting to the share \\NAS\netlogon with the domain administrator, and then you can directly specify the script filename.
- Home: Specify the drive letter and a shared folder that is mapped to the drive letter when the domain user logs on to the domain with the domain username and password. The path specified can be a shared folder name such as /home or /user1profile, or a UNC path such as \\nas.mydomain.local\home.

Groups

To enhance security control, you can create domain user groups. A domain user group is a collection of domain users who share the same access rights to files and folders.

Creating domain user groups

To create a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Click "Create a User Group".
3. Select "Yes" and "Next" to assign domain user(s) to the group or "No" to create a domain group without domain users.
4. Click "Finish".

Deleting domain user groups

To delete a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Select user group(s) and click "Delete".

> **Note:** It is advised not to delete the default existing group of the domain.

Editing group members

To edit domain members within a group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Click the "Edit Group Membership" button under "Action".
3. Select and check domain users to join them to the group or uncheck existing domain users to remove them from the group.
4. Click "Next".

Computers

All computers that have already joined the domain will be listed here, and with permissions granted, they can access the list of domain resources (such as the domain users and groups.) The computer accounts are created automatically after the computers or NAS joins the domain, and administrators can manually create or delete computer accounts.

Creating computer accounts

To create a domain computer account, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Computers" tab.
2. Click "Create a Computer".
3. Fill out the computer name, description and location and click "Next".
4. Choose the group(s) for the computer account and click "Next".
5. Click "Create".

Deleting computer accounts

To delete a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Select the computer account(s) and click "Delete".
3. Click "Delete".

Computer account management

Refer to the following table for available buttons under "Action" and their explanations:

Button	Name	Description
	Edit Computer Properties	Edit the description and location of the computer account.
	Edit Group Members hip	Choose to add the computer account to the user group(s) or remove it from the user group(s).

DNS

The Domain Name System, or DNS, can help the domain controller locate services and devices within the domain (or vice versa) using service and resource records. Two DNS zones are created by default (the domain created when you first set up the NAS as the domain controller and the zone with a name starting with _msdcs.) System administrators can modify DNS settings, add/delete domains, and add/delete records.

Modifying DNS settings

To edit a DNS setting, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password, and the DNS settings will appear. Follow the steps below:

1. Click the setting to be modified
2. Edit the properties of the setting (type and value), adjust the order of the value with the green up-arrow or down-arrow button, or delete the value with the red "X" button.
3. Click "Apply" to save the changes.

Adding domains

To add a domain, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Click "Action" > "Add Domain".
2. Enter the domain name and click "Create".

Adding records

To add a record, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Select a domain
2. Click "Action" > "Add Record".
3. Enter the record properties and click "Create".

> **Note:** Only the following types of records are supported: A, AAAA, PTR, CNAME, NS, MX, SRV, TXT.

Deleting domains or records

To delete a record, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Select a domain or record
2. Click "Action" > "Delete".
3. Click "Yes".

Backup/Restore

The domain controller status can be backed up or restored using the backup/restore function. Only the first domain controller needs to be backed up. In an AD environment where more than one domain controller presents, there are some restrictions and limitations associated with the restore procedures. Please check the restore function carefully.

Backing up domain controllers

To back up the domain controller status, follow the steps below:

1. Go to "Control Panel", Privilege Settings" > "Domain Controller" > "Backup/Restore tab"
2. Check "Back up Database" and set the backup frequency, starting time, destination folder and backup options (choose to overwrite existing backup file or create a new file.)
3. Click "Apply"

Restoring domain controllers

Please note that the current settings, including users, groups and domain controller settings, will be overwritten and all changes made since the last backup will be lost. So, please be specially careful when you restore domain controllers.

To restore the domain controller in a single domain controller environment, follow the steps below:

1. Go to "Control Panel", Privilege Settings" > "Domain Controller" > "Backup/Restore tab" > scroll down to the "Restore ADDC Database" section.
2. Click "Browse" and select the backup file.
3. Click "Import".

If the domain controller you try to restore is in an environment with more than one domain controllers, do not restore from the backup, as this will corrupt the domain controller database. Simply add the NAS back as a domain controller, and it will synchronize with the existing domain controller. If no other domain controllers are online, restore only the first domain controller, and join the other NAS servers as the domain controller back. To restore a domain to a previous state with multiple domain controllers, first disable the domain controller feature on all NAS servers, restore only the first domain controller, and join the other NAS servers as domain controller back.

Network & File Services

Go to "Control Panel" > "Network & File Services" to configure the NAS network settings.
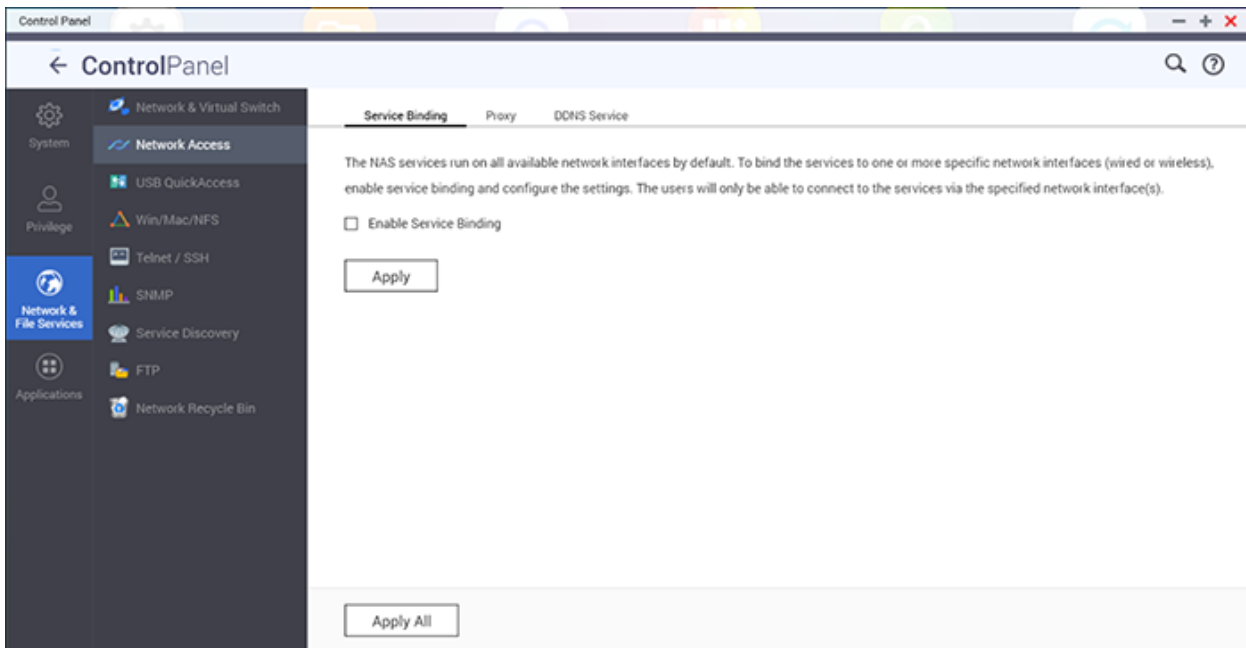
For setup details, refer to the following links:
- Network & Virtual Switch
- Network Access
- USB QuickAccess (Only available for certain models)
- Win/Mac/NFS
- Telnet/SSH
- SNMP
- Service Discovery
- FTP
- Network_Recycle_Bin

Network & Virtual Switch

Go to "Control Panel" > "Network & File Services" > "Network & Virtual Switch" to configure the NAS network settings.
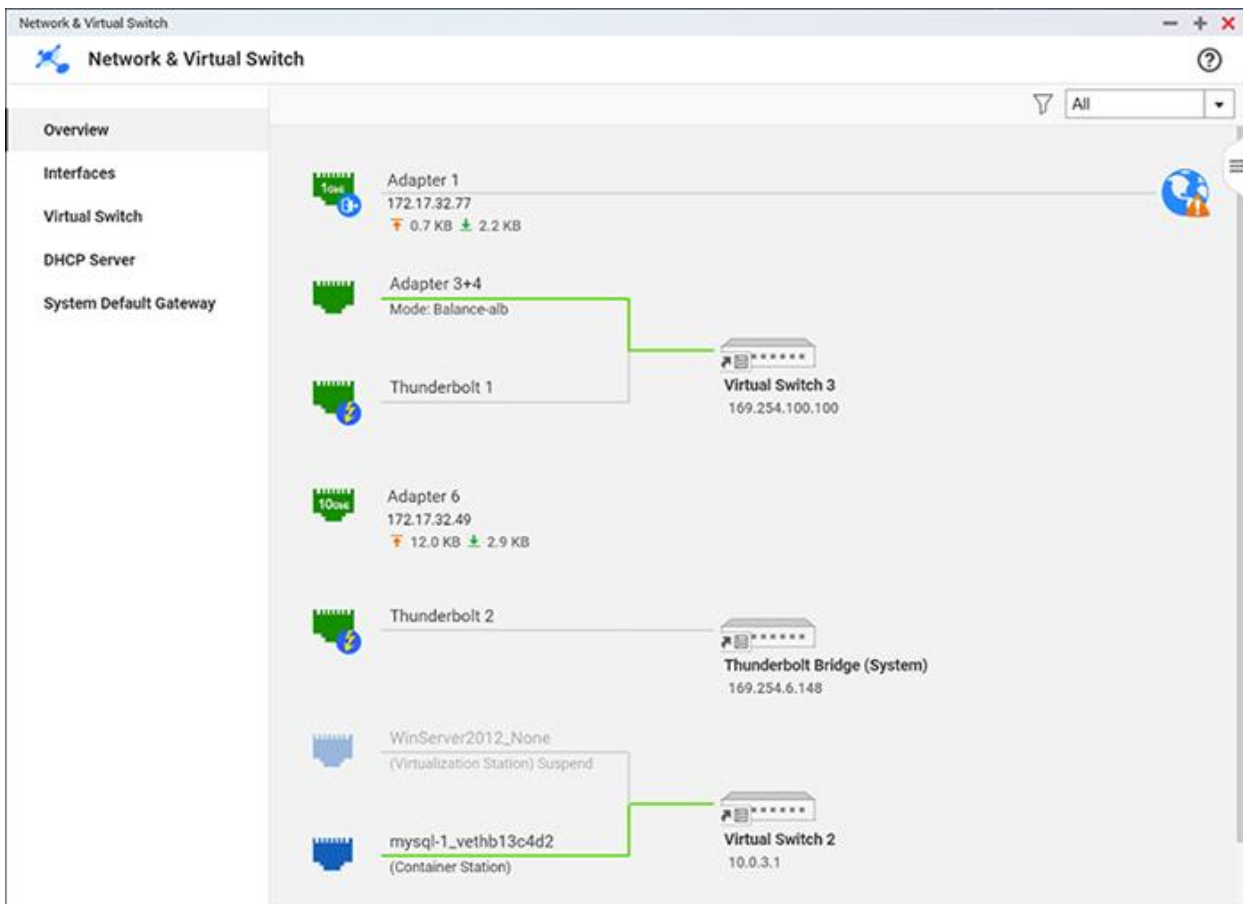
Network & Virtual Switch

Network & Virtual Switch integrates physical interface management, virtual adapters (VMs and containers), Wi-Fi, DHCP server, default gateway, IPv6, and Thunderbolt features. It also supports virtual switches that can bridge 1 Gigabit and 10 Gigabit environments just like using physical switches. You can bridge 1GbE devices and the NAS via virtual switches, and also bridge your NAS and 10GbE environment for file access from the NAS or remotely from the Internet.
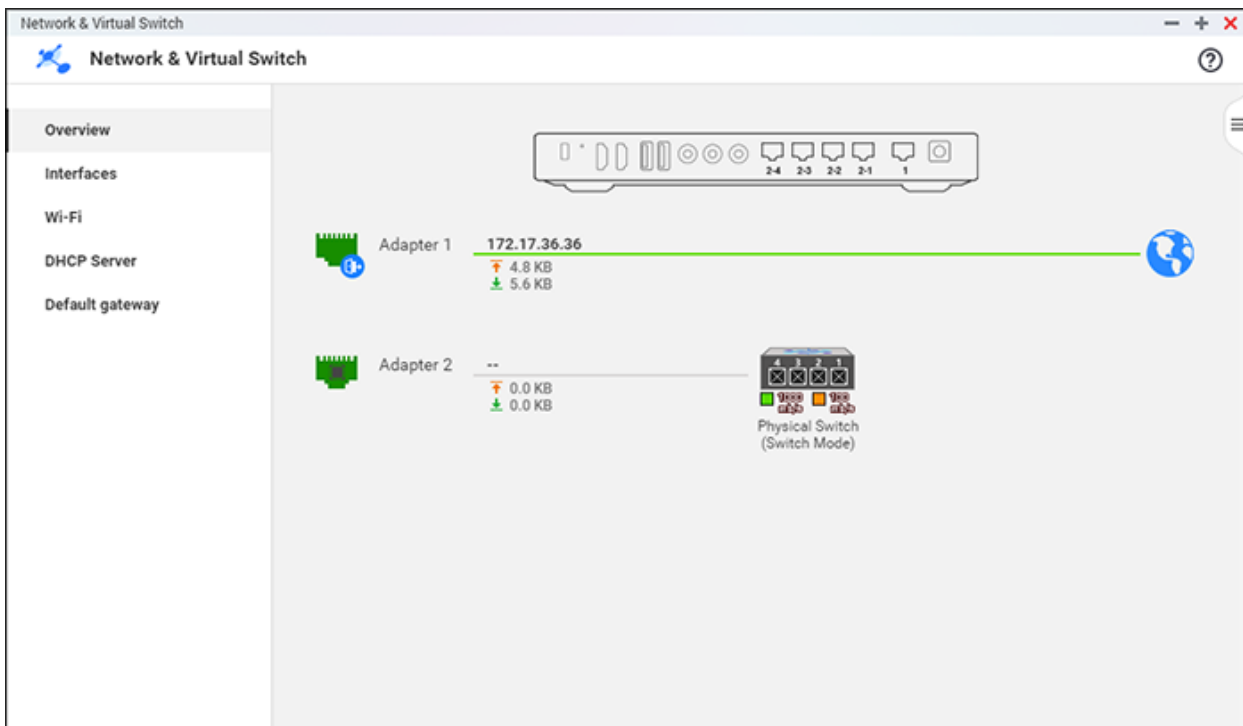
> **Note:** These functions or their content are only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website. The topology may vary among different models.

Overview

This page provides a general overview on the network and you can check the network topology, its status, and each device on the network.

Interfaces

You can edit physical interfaces, virtual switches, DNS server, port trunking, IPv6 and VLAN settings on this page.

Physical interfaces

Physical interfaces are LAN ports on the NAS. To set physical interfaces, click the "interfaces" tab on the left menu of the Network & Virtual Switch window, and choose to configure a physical interface's settings, view its details, or renew its IP address. After you click the "Configure" next to an adapter, you can edit the following values:

- IPv4:
  - Obtain the IP address settings automatically via DHCP: If the network supports DHCP, select this option and the NAS will automatically obtain the IP address and network settings.
  - Use static IP address: To use a static IP address, select this option and enter the IP address, subnet mask, and default gateway. For a NAS with mulitple LAN ports, users

can connect the network interfaces to different switches and configure the TCP/IP settings. The NAS will acquire an IP address for each connected interface, which can access a subnet for each IP. This is known as multi-IP settings*. When using Qfinder Pro to detect the NAS IP, the IP of Ethernet 1 will only be shown in LAN 1 and the IP of Ethernet 2 will only be shown in LAN 2, etc. You can choose to use port trunking for multiple LAN connections.

o Jumbo Frame: "Jumbo Frames" refers to 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. The NAS uses standard Ethernet frames (1500 bytes) by default. If your network appliances support Jumbo Frames, select the appropriate MTU value for the network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.

> **Note:**
> - To use Jumbo Frames, all of the connected network appliances must enable Jumbo Frames and use the same MTU value.
> - Jumbo Frame is only supported by certain NAS models. Refer to the software specification page on the QNAP website for further details. Some NICs only support 1500 and the max speed of some NICs is 8096.

o Network Speed: Select the network transfer rate according to the network environment of the NAS. Select auto-negotiation and the NAS will automatically select the transfer rate. The Network Speed field is not shown for 10GbE & 40GbE adapters and is automatically set to auto-negotiation.

- VLAN: A Virtual LAN (VLAN) is a group of hosts which communicate as if they were attached to the same broadcast domain even if they are located in different physical locations. The NAS can join a VLAN and be configured as a backup storage of other devices on the same VLAN. To join a VLAN, select "Enable VLAN (802.1Q)" and enter the VLAN ID (a value between 1 and 4094.) Keep the VLAN ID safe and make sure the client devices are able to join the VLAN. If you forget the VLAN ID and cannot connect to the NAS, you will need to reset the network settings by pressing the NAS reset button. Once the NAS is reset, the VLAN feature will be disabled. If the NAS supports two Gigabit LAN ports and only one network interface is configured to enable VLAN, you can also connect to the NAS via the other network interface.

> **Note:** The VLAN feature is only supported by x86-based NAS models.

DNS Server

A DNS (Domain Name System) server translates between a domain name (such as google.com) and an IP address (74.125.31.105). On this page, you can configure the NAS to obtain a DNS server address automatically or to specify the IP address of a DNS server. If you choose to specify the IP address, fill out the following fields:

o Primary DNS Server: Enter the IP address of the primary DNS server.

o Secondary DNS Server: Enter the IP address of the secondary DNS server.

Note:

- 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 (BT download, etc) enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.

Port Trunking

The NAS supports Port Trunking which combines two or more Ethernet interfaces to increase bandwidth and offers load balancing and fault tolerance (also known as failover.) Load balancing is a feature that distributes workloads evenly across multiple Ethernet interfaces for higher redundancy. Failover ensures that the network connection will remain available even if a port fails.

To use Port Trunking on the NAS, make sure at least two LAN ports of the NAS have been connected to the same switch and the relevant settings (IP address, network speed, jumbo frame, VLAN, DHCP Server) have been configured.

Follow these steps to configure Port Trunking on the NAS:

1. Go to "Control Panel" > "Network & File Services" > "Network & Virtual Switch" > "Interfaces". Click "Port Trunking", then click "Add".

2. Select the interfaces for a trunking group (for example, adapter 1+2, adapter 3+5+7, or adapter 4+6+8+10).

3. Select "Warn me if a network cable is disconnected from the trunking group" to enable warning messages for this trunking group.

4. Select type of switch being used: directly connecting two NAS without a switch (VJBOD), general switch (most common), or managed switch (supports Port Trunking/LACP). Click "Next".

5. Select a Port Trunking mode. See the Port Trunking options table below for option details. Select "Apply".

> **Note:**
> - Make sure the Ethernet interfaces are connected to the correct switch and the switch has been configured to support the Port Trunking mode selected on the NAS.
> - Port Trunking is only available for NAS models with two or more LAN ports and certain models only provide one Giga LAN port and therefore do not support dual LAN configuration or Port Trunking.

The Port Trunking options available on the NAS:

Field	Description	Switch Required
Balance-rr [Round-Robin](Supported by Direct connection between 2 NAS or using a managed switch)	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 (Supported by using general switch)	Active Backup only uses 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-tlb [Adaptive Transmit Load Balancing] (Supported by using general switch)	Active-Backup only uses 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-alb [Adaptive Load	Balance-alb is similar to balance-tlb but also attempts to redistribute incoming (receive load balancing) for IPV4 traffic. This setup does not	General switches

Balancing] (Supported by using general switch)	require any special switch support or configuration. The receive load balancing is achieved by ARP negotiation sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the Ethernet interfaces in the bond such that different peers use different hardware address for the server. This mode provides load balancing and fault tolerance.	
Balance-xor (Supported by using managed switch)	Balance-xor balances traffic by splitting up outgoing packets between the Ethernet interfaces, using the same one for each specific destination when possible. It transmits based on the selected transmit hash policy. The default policy is a simple slave count operating on Layer 2 where the source MAC address is coupled with destination MAC address. Alternate transmit policies may be selected via the xmit_hash_policy option. Balance XOR mode provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
Broadcast (Supported by using managed switch)	Broadcast sends traffic on all network interfaces. This mode provides fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
802.3ad dynamic [Dynamic Link Aggregation] (Supported by using managed switch)	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. Select the desired hash policy for 802.3ad trunking: Layer 2 (MAC) – Compatible with all managed	Supports 802.3ad LACP (802.1AX-2008)

switches (default).

Layer 2+3 (MAC+IP) – Not supported by all switches. If supported, offers better performance (recommended).

As an example, refer to the following table for Port Trunking modes and their recommended scenario:

Scenario	Recommended Mode	Remark
(1) Directly connect two NAS without a switch (for VJBOD) 	Balance-rr	For VJBOD only.
(2) General Switch 	Active-Backup ; Balance-tlb; Balance-alb	General switches
(3) Managed Switch which supports Port Trunking/LACP 	Balance-rr; Balance-xor; Broadcast; 802.3ad dynamic	The switch must be configured before setting up Port Trunking.

To delete a Port Trunking group, first select a group from the list and click "Delete".

To be automatically notified if a network cable has been disconnected, check "Warn me if a network cable is disconnected from the trunking group" on this page.

IPv6

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

- CIFS/SMB
- AFP
- NFS
- FTP

- iSCSI
- Web Server
- QTS Desktop
- RTRR
- SSH
- Qsync for Windows
- Netbak Replicator

To use this function, select the option "Enable IPv6" and click "Apply". The NAS will restart. After the system restarts, go to the IPv6 page. The settings of the IPv6 interface will be shown. Click the "Edit" button to edit these settings:

- **IPv6 Auto Configuration:** If an IPv6 enabled router is available on the network, select this option to allow the NAS to automatically acquire the IPv6 address and configurations.
- **Use static IP address:** To use a static IP address, enter the IP address (e.g. 2001:bc95:1234:5678), prefix length (e.g. 64), and the gateway address for the NAS. Contact your ISP for the prefix and the prefix length information.
  - Enable Router Advertisement Daemon (radvd): To configure the NAS as an IPv6 host and distribute IPv6 addresses to the local clients that support IPv6, enable this option and enter the prefix and prefix length.
- **IPv6 DNS server:** Enter the preferred DNS server in the upper field and the alternate DNS server in the lower field. Contact the ISP or network administrator for this information. If IPv6 auto configuration is selected, leave the fields as "::".

Thunderbolt

On this page, you can configure Thunderbolt Bridge Addresses, the Thunderbolt interface, and monitor bandwidth usage:

- **Thunderbolt Bridge Address**: This section displays the each Thunderbolt interface along with its connection properties such as associated Virtual Switches, Virtual Switch IP, and associated Thunderbolt JOBDs. A NAS or a JBOD expansion unit can be connected to the Thunderbolt port. If a JBOD expansion unit is connected to the Thunderbolt port, you can view the expansion devices in the Storage Manager.
- **Thunderbolt Bridge (System)**: This section displays the bandwidth usage of the default Thunder bolt interface.

> **Note:** The function or its content is only applicable on some models. To check for applicable models, please refer to the product comparison table on the QNAP website.

USB QuickAccess

USB QuickAccess allows users to directly connect their NAS to their computer using a USB cable and Common Internet File System (CIFS) for using the NAS as a USB storage device. You can perform the following operations using this feature:

- Turn on/off USB QuickAccess: Click the switch icon (to the left of the USB QuickAccess Port icon) to enable/disable USB QuickAccess.
- Choose between DHCP and a static IP address: Click the "Configure" icon and choose whether to obtain the IP address via DHCP or to set a static IP address.
- Set user authentication levels: Click "Authentication" (the icon next to "Configure") to choose an authentication method for the USB QuickAccess port. There are three methods available:
  - All NAS Users: A NAS username and password are required to access files and folders using Qfinder Pro or CIFS.
  - Everyone: No username or password is required to access files and folders using Qfinder Pro or CIFS.
  - Selected Users/Groups: Administrators can choose users/groups to use USB QuickAccess and these users/groups need to enter their username and password before accessing files and folders. With this option, only chosen NAS users/groups (or domain users) can use USB QuickAccess.
- Monitor incoming and outgoing traffic: Monitor the traffic volume of the USB QuickAccess port.

> **Note:**
> - This function (or its content) is only available on certain models.
> - The DHCP server created by USB QuickAccess cannot be disabled, configured or deleted.
> - Besides local user or group accounts, you can also grant access rights to domain users for USB QuickAccess. To do so, please first set up authentication in "Domain Security".
> - For the highest possible speed, connect the NAS to a USB 3.0 port on your computer using a USB 3.0 cable.

Wi-Fi

To connect to a Wi-Fi network, plug a USB Wi-Fi dongle into the NAS, and a list of Wi-Fi access points will be shown. There are two methods to connect to Wi-Fi networks:

- Connecting to an existing Wi-Fi network.
- Manually connecting to a Wi-Fi network.

> **Note:**
> - Wireless connection performance depends on many factors such as the adapter model, the USB adapter's performance, and the network environment. Wired connections will always provide greater stability and performance.
> - The system only supports one USB Wi-Fi dongle at a time.
> - For a list of compatible USB Wi-Fi dongles, visit http://www.qnap.com/compatibility and select "USB Wi-Fi".
> - This feature is not supported by the TS-269H.

Method 1: Connecting to an existing Wi-Fi network:

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

Icon / Option	Name	Description
Rescan	Rescan	Search for Wi-Fi networks in range.
🔒	Secured network	The Wi-Fi network requires a network key.
▶	Connect	Connect to a Wi-Fi network. If a security key is required, you will be prompted to enter the key.
✎	Edit	Edit the connection information. You can select to automatically connect to the Wi-Fi network.
■	Disconnect	Disconnect from the Wi-Fi network.
✖	Remove	Delete the Wi-Fi network profile.
Show all	Show all	Display all available Wi-Fi networks. Deselect this option to only show configured network profiles.

Click "Rescan" to search for available Wi-Fi networks. Select a Wi-Fi network to connect to and click "Connect". Enter the security key if needed. Click "Next" and the NAS will attempt to connect to the wireless network. You can view the status of the configured network profiles.

Message	Description
Connected	The NAS is currently connected to the Wi-Fi network.
Connecting	The NAS is trying to connect to the Wi-Fi network.
Out of range or hidden SSID	The wireless signal is not available or the SSID is not broadcast.
Failed to get IP	The NAS is connected to the Wi-Fi network but could not get an

	IP address from the DHCP server. Check the router settings.
Association failed	The NAS cannot connect to the Wi-Fi network. Check the router settings.
Incorrect key	The entered security key is incorrect.
Auto connect	Automatically connect to the Wi-Fi network. This is not supported if the SSID of the Wi-Fi network is not broadcast.

Method 2: Manually connecting to a Wi-Fi network:

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

You can choose to connect to an ad hoc network in which you can connect to any wireless devices without the need for an access point. To set up, follow these steps:

1. Enter the network name (SSID) of the wireless network and select the security type.
   - No authentication (Open): No security key required.
   - WEP: Enter up to 4 WEP keys and choose 1 key to be used for authentication.
   - WPA-Personal: Choose AES or TKIP encryption and enter the encryption key.
   - WPA2-Personal: Enter a security key.
2. Type in the security key.
3. Click "Finish" after the NAS has added the Wi-Fi network.
4. To edit IP address settings, click "Edit". You can choose to automatically obtain the IP address by DHCP or to set a fixed IP address.

If the Wi-Fi connection is the only connection between the NAS and the router/AP, you must select "WLAN1" as the default gateway in "Network" > "TCP/IP" page. Otherwise, the NAS will be unable to connect to the Internet or communicate with another network.

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

Setting up the TBS-453A

The TBS-453A is the only QNAP NAS model with a built-in physical switch chip for optimized switch performance. For this model, you can connect the network interfaces 2-1~2-4 to a physical switch for network expansion. This model also has two modes: Switch mode and Private Network mode. To set up Switch mode, follow these steps:

1. Connect one of the four ports (Port 2-1 to 2-4) to an external network or a default gateway and connect your local devices to any of the remaining three ports.
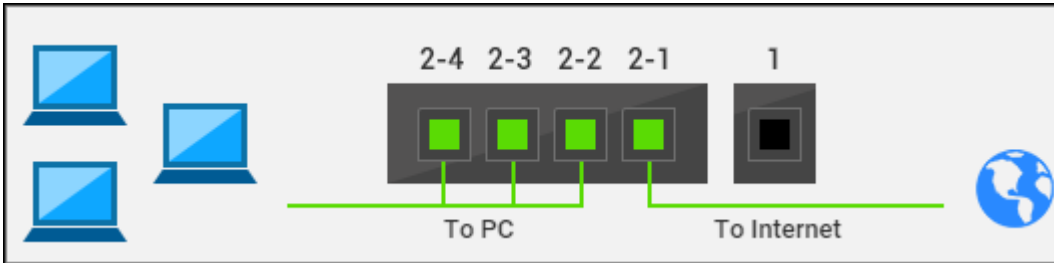
2. Go to "Interfaces" (on the left menu) > "Interfaces" (on top of the page) > click the "switch" icon next to an interface.
3. Select "Switch Mode" > "Apply". Since the default option is Switch mode, if this is your first time setting up this mode, you may skip Steps 2 and 3.

To set up Private Network mode, follow these steps:

1. Make sure that none of the four ports (Port 2-1 to 2-4) is connected to an external network or a default gateway.
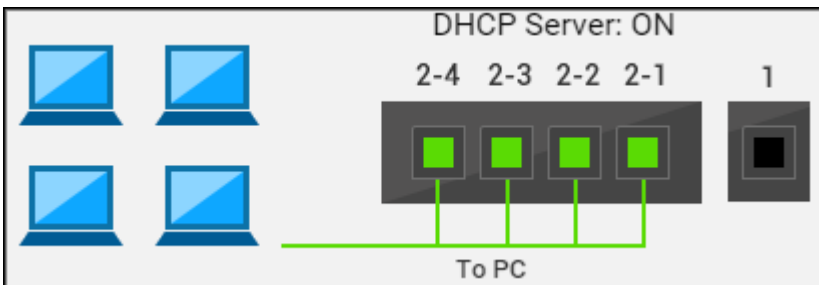
2. Go to "Interfaces" (on the left menu) > "Interfaces" (on top of the page) > click the "switch" icon next to an interface.
3. Select "Private Network Mode" > "Apply".

Note: The Virtual Switch feature is not available on the TBS-485A.

Virtual Switch

Virtual Switches allow physical interfaces (network adapters, Thunderbolt ports) and virtual adapters (VMs and containers) to communicate with each other. For example, with the use of a Virtual Switch, a Virtual Machine, container, and physical adapter be connected to the

Internet. Virtual Switches could also be used to bridge 1 Gigabit, 10 Gigabit, 40 Gigabit, and Thunderbolt environments just as a physical switch could.
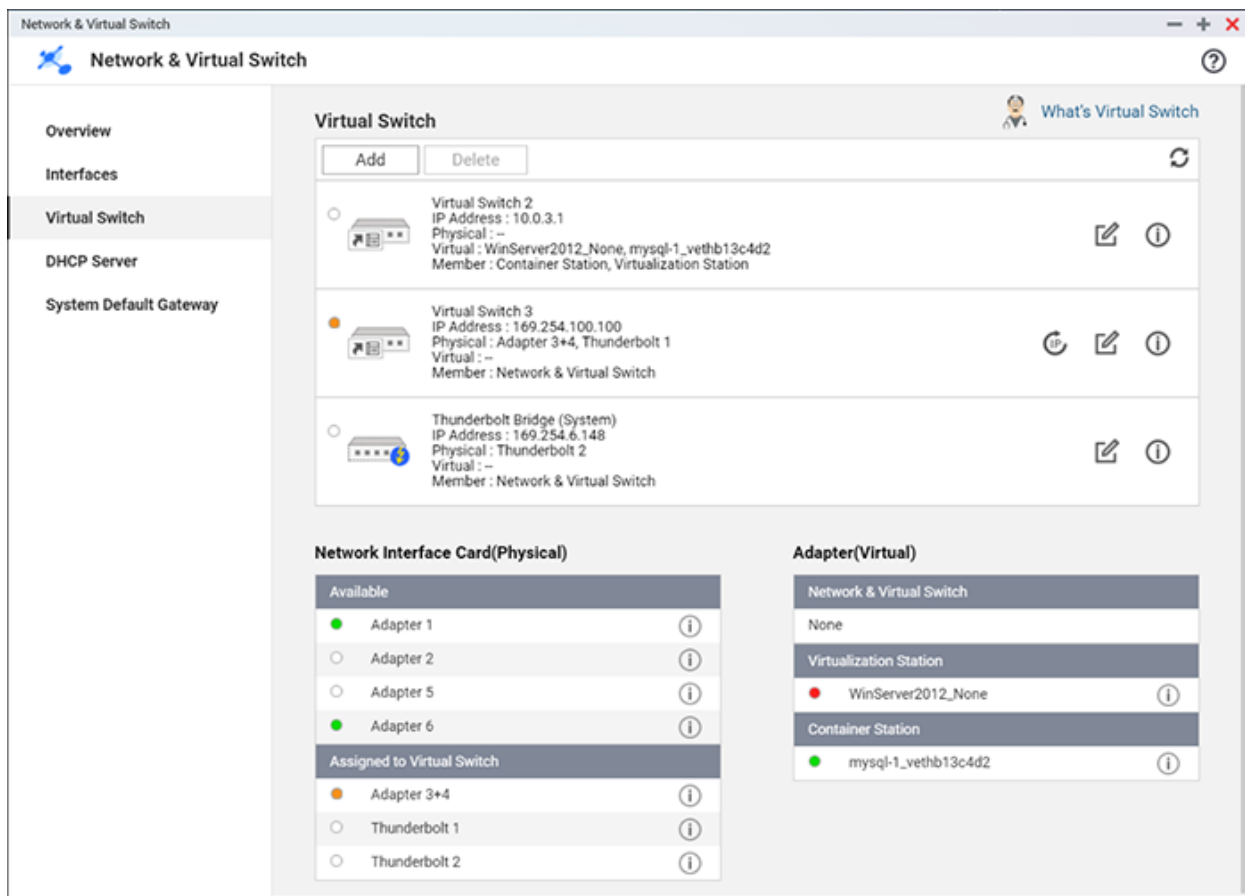
Setting Up a Virtual Switch

To set up a Virtual Switch, go to "Main Menu" > "Network & Virtual Switch" > "Virtual Switch", click "Add". Choose between Basic Mode and Advanced Mode. In Basic Mode will, the Virtual Switch will be automatically assigned an IP address. Advanced Mode allows the user to use a dynamic IP, static IP, or no IP (used for external or isolated networks). Advanced mode also gives the user the option to enable NAT and DHCP server for the virtual switch.

Using Basic Mode:
1. Select Basic Mode in the Create a Virtual Switch window.
2. Select the adapters to connect to the Virtual Switch. It is recommended to enable the Spanning Tree Protocol to avoid bridge loops.
3. Click Apply.

Using Advanced Mode:
1. Select Advanced Mode in the Create a Virtual Switch window.

2. Select the adapters to connect to the Virtual Switch. It is recommended to enable the Spanning Tree Protocol to avoid bridge loops. Click "Next".

3. Choose to use a dynamic, static, or no IP address for the Virtual Switch.

- To use static IP, choose to use the same network settings as another adapter or manually enter the network information by filing in the Fixed IP Address, Subnet Mask, and Default Gateway fields.

4. Click "Next".

5. Select NAT to enable NAT.

> **Note:**
> - NAT cannot be enabled on the default gateway.
> - The IP address of Virtual Switch cannot be in the ranges that do not support IP forwarding (for example, 127.xxx.xxx.xxx, 169.254.xxx.xxx, 192.0.2.xxx, 198.51.100.xxx).
> - Ensure that the IP address of the Virtual Switch is not in the subnet of any other interfaces in use.

6. To enable DHCP server, select "Enable DHCP Server" and fill in the following fields:

- **Start IP, End IP, Subnet Mask, Lease Time**: Set the range of IP addresses allocated by the NAS to the DHCP clients, the subnet mask and the lease time. The lease time refers to the time that an IP address is leased to the clients. During that time, the IP address will be reserved to the assigned client. When the lease time expires, the IP address can be assigned to another client.
- **Default Gateway**: Enter the IP address of the default gateway for the DHCP server.
- **DNS Server**: Specify a DNS server for the DHCP server. Refer to the DNS Server section in this chapter for more information.
- **WINS Server (optional)**: WINS (Windows Internet Naming Service) resolves Windows network computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. Enter the IP address of the WINS server on the network if available.
- **DNS Suffix (optional)**: The DNS suffix is used for resolution of unqualified/incomplete host names.
- **TFTP Server & Boot File (optional)**: The NAS supports PXE booting of network devices. Enter the IP address of the TFTP server and the boot file (including directory on the TFTP server and file name.) For remote booting of devices, enter the public IP address of the TFTP server.

> **Note:** To avoid IP address conflicts, do not enable DHCP server if there is another DHCP server running on the local network or network access errors

7. Click "Next".

8. Confirm the Virtual Switch settings and click "Apply" to continue.

Thunderbolt to Ethernet (T2E)

Thunderbolt to Ethernet functionality allows the Thunderbolt port to act as an Ethernet connection.

There are two methods of setting up Thunderbolt to Ethernet using your NAS. It is recommended that users use Qfinder Pro to set up Thunderbolt to Ethernet.

To set up T2E manually (without Qfinder Pro):

1. Go to Network & Virtual Switch and create a virtual switch with a Thunderbolt (See Set up a Virtual Switch for more information).

2. Optional: Run the following commands in Terminal as an administrator on your MAC to temporarily change your network settings:

   sudo sysctl net.inet.tcp.path_mtu_discovery=0

   sudo sysctl net.inet.tcp.tso=0

Rebooting the Mac will undo these settings.

3. Run the following command in Terminal as an administrator on your MAC to permanently apply the settings:

   sudo bash −c 'printf "#QNAP\nnet.inet.tcp.path_mtu_discovery=0\nnet.inet.tcp.tso=0\n#QNAP\n" >> /etc/sysctl.conf'

This command adds two lines to the sysctl.conf file.

To access the LAN using T2E, set PMTU to 0 (default value is 1):

   net.inet.tcp.path_mtu_discovery=0

To access the Internet, set TSO to 0 (default value is 1):

   net.inet.tcp.tso=0

> **Note:**
> - Qfinder Pro will automatically configure your Mac settings file: /etc/sysctl.conf.
> - T2E Internet functionality reduces the MTU size of packets sent from the Mac and thus affects upload speeds. To revert to the default settings, use Qfinder Pro or Terminal to set net.inet.tcp.tso to 1).
> - T2E with Thunderbolt 2 on Windows may have connectivity issues due to Thunderbolt drivers. This issue does not affect Thunderbolt 3 with Windows.

DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to clients on a network. Select the interface(s) to set the NAS as a DHCP server if there are none on the local network where the NAS is located.

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

To set up a DHCP server on the NAS:

1. Go to "Control Panel" > "Network & File Services" > "Network & Virtual Switch" > "DHCP Server", then click "Add".
2. Select the interface to set as DHCP server. Click "Next".
3. Select to "Enable DHCP server on the original network", "Reassign an IP address to the adapter and enable a DHCP server on a new subnet", or "Enable DHCP server for another subnet". Click "Next".
4. Fill out the fields below:

- **Start IP, End IP, Subnet Mask, Lease Time:** Set the range of IP addresses allocated by the NAS to the DHCP clients, the subnet mask and the lease time. The lease time refers to the time that an IP address is leased to the clients. During that time, the IP address will be reserved to the assigned client. When the lease time expires, the IP address can be assigned to another client.
- **Default Gateway:** Enter the IP address of the default gateway for the DHCP server.
- **DNS Server:** Specify a DNS server for the DHCP server. Refer to the DNS Server section in this chapter for more information.
- **WINS Server (optional):** WINS (Windows Internet Naming Service) resolves Windows network computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. Enter the IP address of the WINS server on the network if available.
- **DNS Suffix (optional):** The DNS suffix is used for resolution of unqualified/incomplete host names.
- **TFTP Server & Boot File (optional):** The NAS supports PXE booting of network devices. Enter the IP address of the TFTP server and the boot file (including directory on the TFTP server and file name.) For remote booting of devices, enter the public IP address of the TFTP server.

5. Click "Apply".

System Default Gateway

You can choose to have the system automatically detect the default gateway or manually set the interface as the default gateway:

- The system will detect adapters that can reach the Internet and set one of these as the default gateway: For connecting to Internet, you can choose this option and the system will choose an adapter that can reach the Internet and set it as the default gateway.

- Manually choose the system's default gateway: Administrators can assign two adapters as the first and second default gateway for failover protection. Both physical adapters and virtual switches can be assigned. To assign the primary and secondary default gateways, tick the option "If this adapter cannot reach the network, the system will use this second priority as the default gateway. Once the first priority is connected, the system will revert to it as the default system gateway". Note that this failover protection option is only available when both of the interfaces on the NAS are connected to the Internet.

Network Access

Go to "Control Panel" > "Network & File Services" > "Network Access".
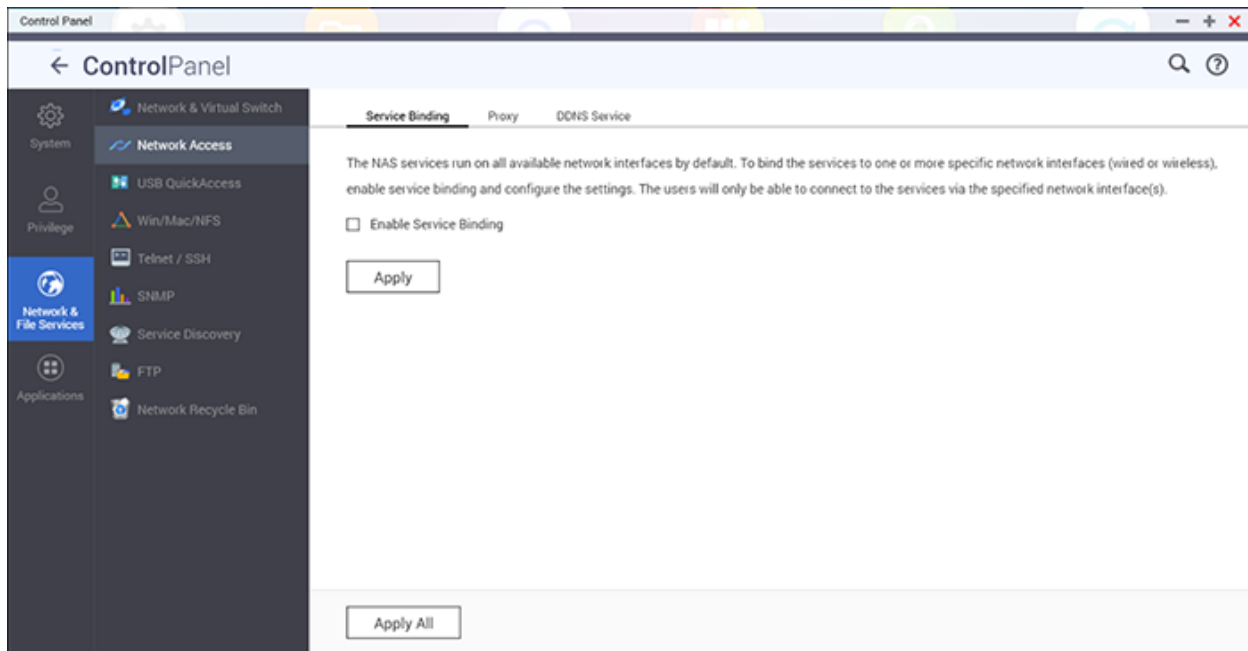
Service Binding

NAS services run on all available network interfaces by default. You can bind services to one or more specific network interfaces. First check "Enable Service Binding" and available network interfaces on the NAS will be shown. Select at least one network interface that each service should be bound to. Then click "Apply". Users will only be able to connect to services via the specified network interfaces. If the settings cannot be applied, click "Refresh" to list the current network interfaces on the NAS and configure service binding again.

> **Note:**
> - Service binding is only available for NAS models with multiple network interfaces (wired and wireless).
> - Service binding is not available for network interfaces that are connected to virtual switches.
> - After applying service binding settings, the connection of currently-online users will be kept even if they were not connected to services via the specified network interfaces. The specified network interfaces will be used for the next connected session.

Proxy

To allow the NAS to access the Internet through a proxy server to update the firmware, get new virus definitions, and to download Apps, first enable this service and enter the proxy server settings.

DDNS Service

To allow remote access to the NAS using a domain name instead of a dynamic IP address, enable the DDNS service.
The NAS supports the DDNS providers: http://www.dyndns.com, http://update.ods.org, http://www.dhs.org, http://www.dyns.cx, http://www.3322.org, http://www.no-ip.com, http://www.Selfhost.de, http://www.oray.com.

> **Note:** Some of these DDNS services are not free.

> **Additional Reference:**
> - How to set up proxy server on QNAP Turbo NAS for optimized website access.
> - Set up DDNS Service for Remote Internet Access to QNAP NAS.

Win/Mac/NFS

Go to "Control Panel" > "Network & File Services" > "Win/Mac/NFS" to configure networking services.

In this chapter, the following topics are covered:

- Microsoft Networking
- Apple Networking
- NFS Service

Microsoft Networking

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

Standalone Server

Use local users for authentication. The NAS will use local user account information (created in "Privilege Settings" > "Users") to authenticate users who access the NAS.

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

AD Domain Member

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

LDAP Domain Authentication

Use an LDAP directory to authenticate the users. To use this option, enable LDAP authentication and specify the settings in "Privilege Settings" > "Domain Security". When this option is enabled, you need to select either the local NAS users or the LDAP users that can access the NAS via Microsoft Networking.

Advanced Options

- **WINS server:** If you have a WINS server on your network and want to use this server, enter the WINS server IP. The NAS will automatically register its name and IP address with the WINS service. Do not enable this option if you are unsure about the settings.
- **Local Domain Master:** A Domain Master Browser is responsible for collecting and recording resources and services available for each PC on the network or a workgroup of Windows. When you find the waiting time for loading network resources to be too long, it may be caused by a 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 enable this option if you are unsure about the settings.
- **Allow only NTLMv2 authentication:** NTLMv2 stands for NT LAN Manager version 2. When this option is enabled, login to the shared folders by Microsoft Networking will only be allowed using NTLMv2 authentication. If the option is disabled, NTLM (NT LAN Manager) will be used by default and NTLMv2 can be negotiated by the client. The default setting is disabled.
- **Name resolution priority:** You can select to use DNS server or WINS server to resolve client host names from IP addresses. When you set up your NAS to use a WINS server or to be a WINS server, you can choose to use DNS or WINS first for name resolution. When WINS is enabled, the default setting is "Try WINS then DNS". Otherwise, DNS will be used for name resolution by default.
- **Login style: DOMAIN\USERNAME instead of DOMAIN+USERNAME for FTP, AFP, and File Station:** In an Active Directory environment, the default login formats for the domain users are:
  o Windows shares: domain\username
  o FTP: domain+username
  o File Station: domain+username
  o AFP: domain+username

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

- **Automatically register in DNS:** When this option is enabled and the NAS is joined to an Active Directory, the NAS will automatically register itself in the domain DNS server. This will create a DNS host entry for the NAS in the DNS server. If the NAS IP changes, the NAS will automatically update the IP in the DNS server.
- **Enable trusted domains:** Select this option to load users from trusted Active Directory domains and specify their NAS access permissions in "Privilege Settings" > "Shared Folders". Domain trusts are only set up in Active Directory, not on the NAS.)
- **Enable Asynchronous I/O:** Enable this option to increase SAMBA performance. Please note: we strongly recommend using a UPS when this option is enabled.
- **Enable Highest SMB version:** Please choose the version of the SMB protocol (Server Message Block) for your Microsoft Networking operations. If you are unsure, please use the default option.

Apple Networking

To connect to the NAS from Mac OS X, enable Apple Filing Protocol. If the AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the NAS. Enter an asterisk (*) to use default settings. This setting is disabled by default. To allow access to the NAS from Mac OS X 10.7 Lion, enable "DHX2 authentication support". Click "Apply" to save the settings. You can use the Finder to connect to a shared folder from Mac. Go to "Go" > "Connect to Server", or simply use the default keyboard shortcut "Command+k". Enter the connection information in the "Server Address" field, such as "afp://*YOUR_NAS_IP_OR_HOSTNAME*". Here are some examples:
- afp://10.8.12.111
- afp://NAS-559
- smb://192.168.1.159

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

NFS Service

To connect to the NAS from Linux, enable the NFS service under NFS. Select "Enable NFS v2/v3 Service" for NFS version 2 or 3. Select "Enable NFS v4 Service" for NFS version 4. Multiple selections can be selected. To configure NFS access rights to shared folders on the NAS, go to "Privilege Settings" > "Share Folders" and click the Access Permission button on the "Action" column. Select NFS host access from the drop-down menu on the top of the page and specify the access rights. For either the "read/write" or "read-only" option, you can specify the IP address or domains that are allowed to connect to the folder by NFS.

- read/write: Allow users to create, read, write, and delete files or folders in the shared folder and any subdirectories.
- read-only: Allow users to read files in the shared folder and any subdirectories but they are not allowed to write, create, or delete any files.

Connecting to the NAS by NFS
On Linux, run this command:

> **mount -t nfs <NAS IP>:/<Shared Folder Name> <Directory to Mount>**

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

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

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

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

Telnet/SSH

Enable this option to connect to the NAS by Telnet or SSH encrypted connection (only the "admin" account can remotely log in.) Use Telnet or SSH connection clients such PuTTY to connect to the NAS. Ensure the specified ports have been opened on the router or firewall.

After enabling this option, you can access this server via Telnet or SSH connection.

Note: Only the account admin can login remotely.

☐ Allow Telnet connection (Only the account admin can login remotely.)

Port number: 13131
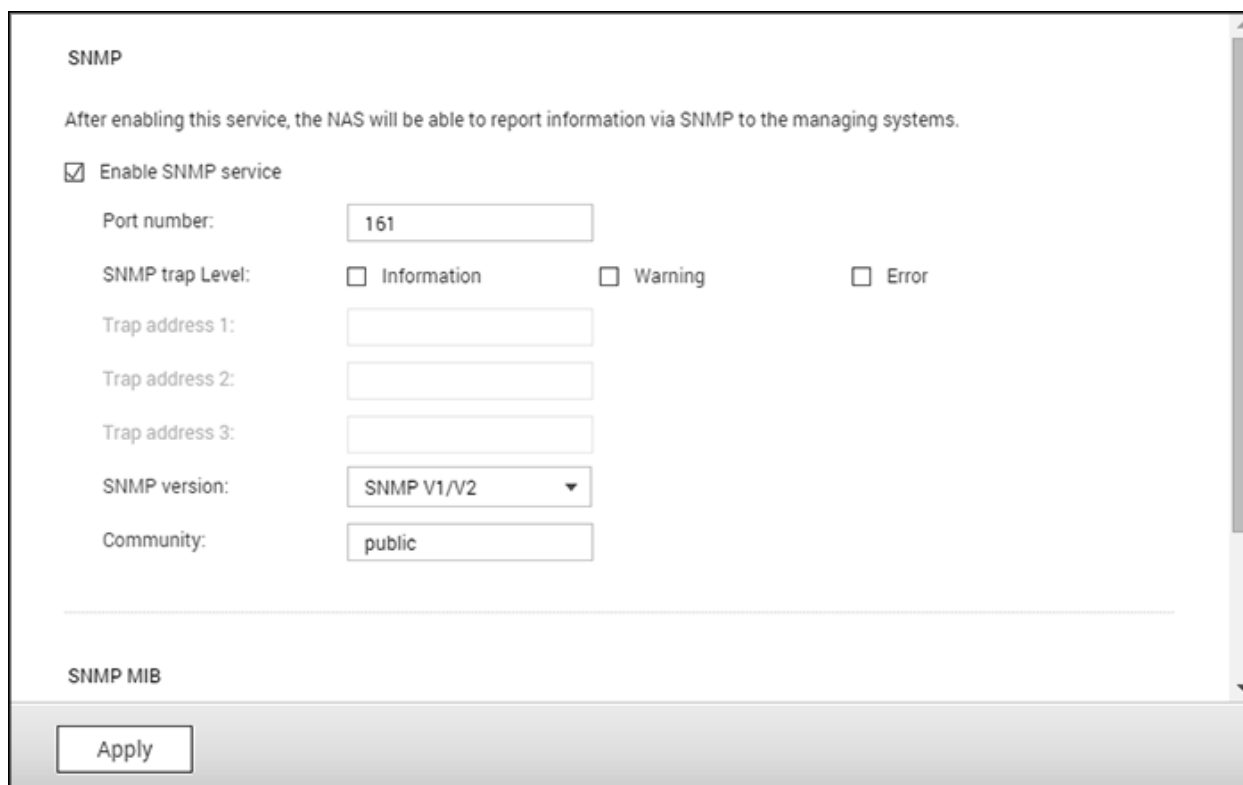
☑ Allow SSH connection (Only administrators can login remotely.)

Port number: 22

☑ Enable SFTP

Edit Access Permission

Apply

To use SFTP (SSH File Transfer Protocol/Secure File Transfer Protocol), ensure that the option "Allow SSH connection" has been enabled. You can click "Edit Access Permission" to choose which administrators can access the NAS via SSH connections.

SNMP Settings

Enable SNMP (Simple Network Management Protocol) on the NAS and enter the trap address of the SNMP management stations (SNMP manager) - for example, a PC with SNMP software installed. When an event, warning, or error occurs on the NAS, it will report a real-time alert to SNMP management stations.
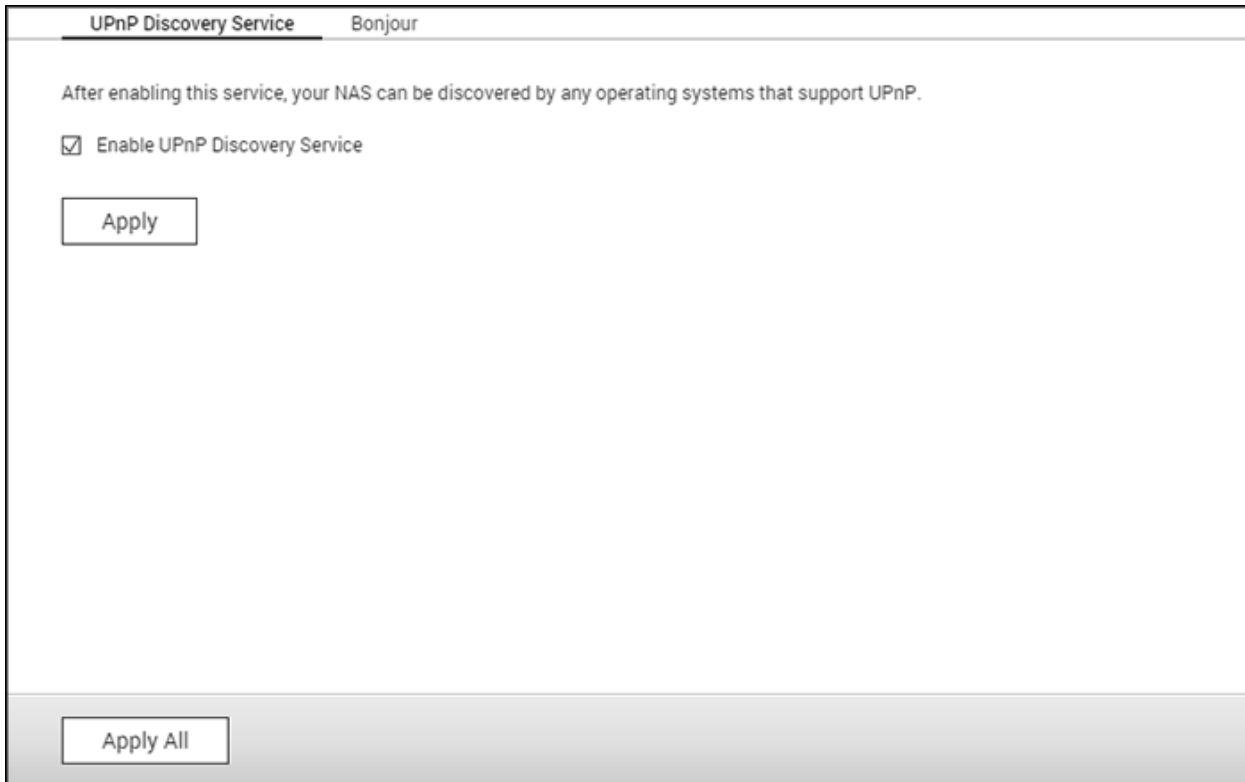
The fields are described as below:

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

	management station and the NAS. The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
SNMP V3	The NAS supports SNMP version 3. Specify the authentication and privacy settings if available.

Service Discovery

Go to "Control Panel" > "Network & File Services" > "Service Discovery" to configure the UPnP discovery service and Bonjour.

UPnP Discovery Service

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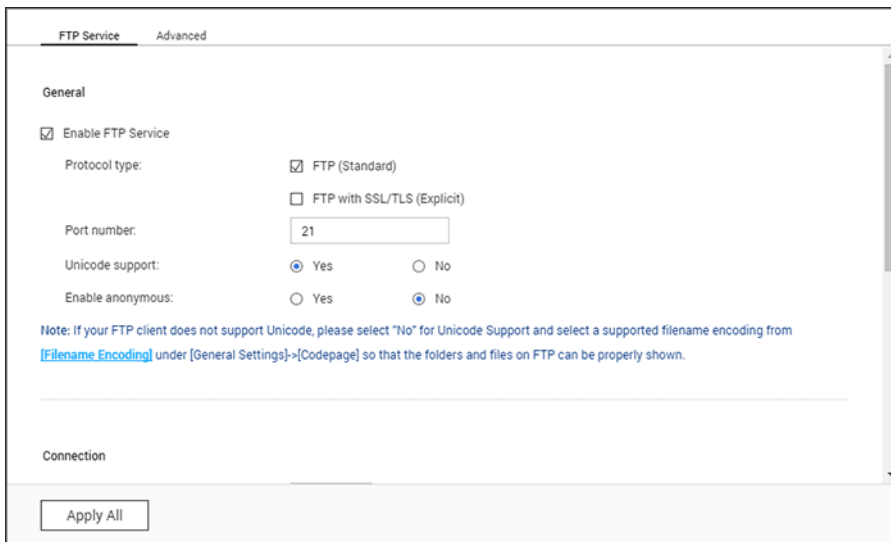
Bonjour

By using Bonjour, your Mac will automatically discover network services (such as FTP) running on the NAS without needing to enter IP addresses or configuring DNS servers.

Note: You must activate the services on their setup pages and then enable them in this section so that the NAS can advertise them using Bonjour.

FTP

Go to "Control Panel" > "Network & File Services" > "FTP" to Configure the FTP server.

FTP Service

When you enable the 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 a browser and enter ftp://NAS IP:Port. Enter the username and the password to login the FTP service.

- **Protocol Type:** Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the correct protocol type in your client FTP software to ensure successful connection. Multiple selections can be selected.
- **Port number:** Specify the port number of the FTP service.
- **Unicode Support:** Toggles Unicode support. The default setting is No. If your FTP client does not support Unicode, it is recommended to disable this option and select the specified language in "Control Panel" > "General Settings" > "Codepage" so that the file and folder names can be correctly displayed. If your FTP client supports Unicode, enable this option for both your client and NAS.
- **Enable Anonymous:** Enable this option to allow anonymous access to the NAS by FTP. Anonymous users can connect to files and folders which are open for public access. If this option is disabled, users must enter an authorized username and password to connect to the NAS.
- **Connection:** Enter the maximum number of allowed FTP connections for the NAS and a single account and check "Enable FTP transfer limitation" to specify the maximum upload and download rates.

- **Online Users:** Check details of the current FTP connections, including the type of connection, login date, login time, user account, source IP, and computer name.

Note: The maximum number of FTP connections varies based on the size of RAM installed on the NAS:
- If the NAS memory =< 1 GB, the maximum is 256.
- If the NAS memory = 2 GB, the maximum is 512.
- If the NAS memory >= 3 GB, the maximum is 1024.
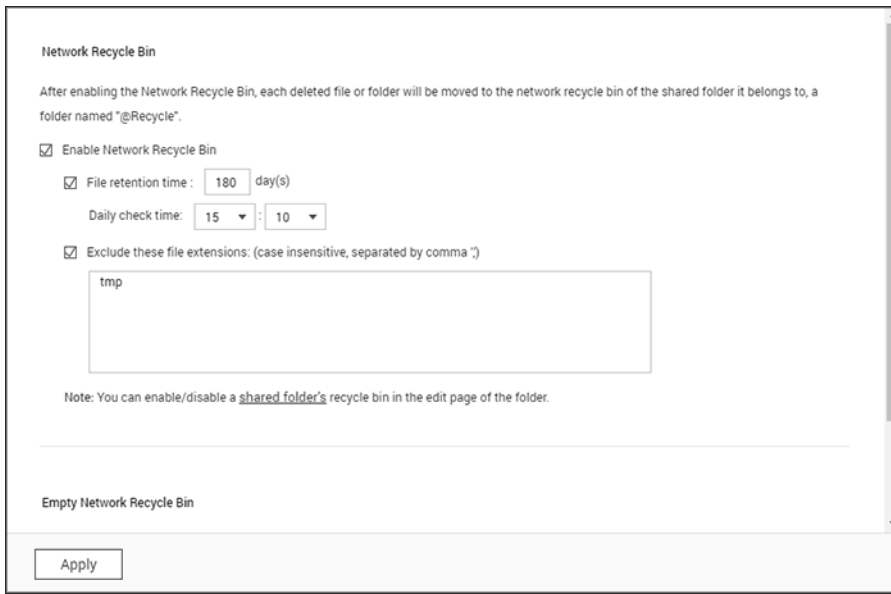
Advanced

- **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.
- **Respond with external IP address for passive FTP connection request:** Enable this function when a 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. When this is enabled, the NAS replies with the specified IP address or automatically detects an external IP address so that the remote computer is able to connect to the FTP server.
- **Set root directory:** After enabling this function and selecting a root directory, only that directory will be visible to FTP users. Otherwise, all of the shared folders will be visible.

Network Recycle Bin

The Network Recycle Bin retains files deleted on the NAS. Within each shared folder, a dedicated folder with the name @Recycle is created after the initial QTS installation. Specify the number of days (1-180) to retain files and the daily time. You can also specify the file extensions to be excluded from the bin. This feature only supports file deletion via Samba, AFP, FTP and File Station.

Using Network Recycle Bin

- To delete all the files in the bin, click "Empty All Network Recycle Bin".
- To recover deleted files from the Network Recycle Bin, right click on the files in the @Recycle folder and select "RECOVER".
- To permanently delete a file in the recycle bin, right click on the file in the @Recycle folder and select "Del (from recycle)".
- To empty the recycle bin for an individual shared folder, right click inside the recycle bin and select "Empty Recycle Bin".

Restricting Access to Network Recycle Bin
The Network Recycle Bin can be restricted to administrators usage by going to "Control Panel" > "Privilege Settings" > "Shared Folders". Click "Property" under "Action" for the shared folder to be configured and check "Restrict the access of Recycle Bin to administrators only for now".

Caution: **All of the files in network recycle bins will be permanently deleted when files are deleted in "@Recycle" on the network share or when you click "Empty All Network Recycle Bins".** The Network Recycle Bin feature is not supported for USB/eSATA external storage devices and virtual disks.

Business Applications

The following NAS functions are designed to meet business needs.
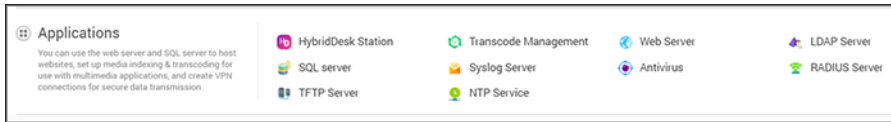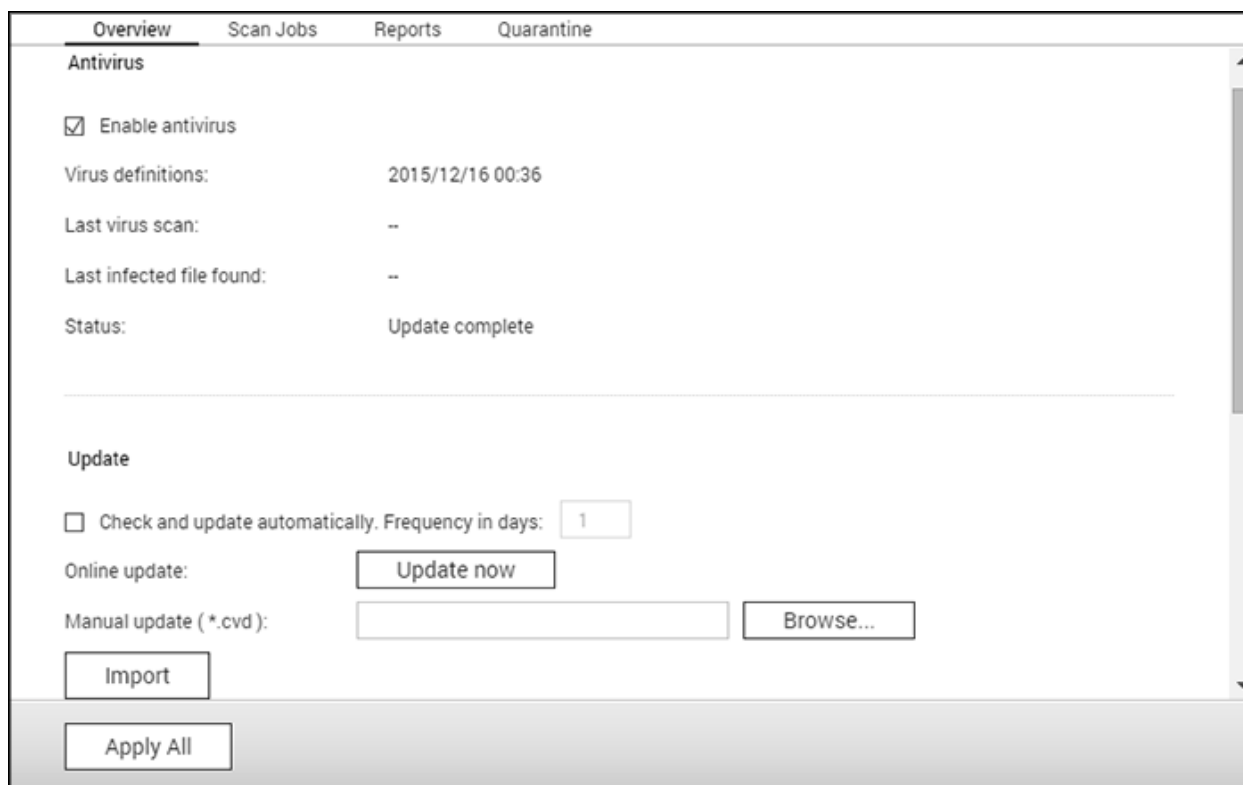
For setup details, refer to the following links:

- Antivirus
- Backup Station
- File Station
- iSCSI Service
- LDAP Server
- QVPN
- SQL Server
- NTP Service
- RADIUS Server
- Syslog Server
- TFTP Server
- Virtualization
- Web Server

Antivirus

Configure antivirus features on this page.

Overview

- Antivirus: Use the antivirus to scan the NAS manually or on recurring schedules. It will delete, quarantine, or report files infected by viruses, malware, Trojans, and other malicious threats. To use this feature, select "Enable antivirus" and click "Apply".
- Update: Select "Check and update automatically" and specify the intervals in days to automatically update the antivirus definitions. Click "Update Now" to check for new antivirus definitions and to update if necessary. Users can also download updated definitions from http://www.clamav.net and manually update the antivirus definitions. The NAS must be connected to the Internet to use this feature.
- Quarantine: View the quarantine information of the disk volumes on the NAS. For more details, go to "Applications" > "Antivirus" > "Quarantine".

Note: The antivirus engine selector next to the "Enable antivirus" checkbox is only available after an additional antivirus App has been installed from the App Center.

Scan Jobs

The NAS supports manual and scheduled scanning of all or specific shared folders. Up to 64 schedules can be created and up to 5 scan jobs can run concurrently. To create a scan job, follow these steps.

1. Go to "Applications" > "Antivirus" > "Scan Jobs". Click "Add a Scan Job".

2. Enter the job name and select the shared folders to scan. To scan a specific shared folder, select the share and click "Add".

3. Multiple shared folders can be selected. To remove a shared folder, click the "Delete (X)" button next to the share name and click "Next". Define the scan job schedule and click "Next".

4. Select to scan all the files in the shared folder(s) or quick scan to scan only potentially dangerous files. Select "Exclude files or folders" and specify a file, a folder, or a file extension to be excluded from the virus scan and click "Next". Separate each entry with a space in the same line or enter one entry per line. For example:
   o /Public/testfile.txt
   o /Download
   o *.log
   o *.exe *.com
   o *.txt; click "Next".

5. Enable other scan options and click "Next":
   o Specify the maximum file size (1-4096 MB) allowed for scanning.
   o Enable "Scan compressed files" to include these files in shared folders. Specify the maximum amount of data (1-4096 MB) in a compressed file for scanning (if applicable).
   o The maximum file size and maximum compressed file size may vary based on the NAS model and available memory.
   o To scan MS Office and Mac Office files, RTF, PDF, and HTML files, select "Deep scan for document files".

6. Specify the actions to take when infected files are discovered and click "Finish" to create the scan job.
   o Only report the virus: The virus scan reports are recorded under the "Reports" tab. No actions will be taken for the infected files.
   o Move infected files to quarantine: The infected files will be quarantined and cannot be accessed from their original shared folders. Users can view the virus scan reports under the "Reports" tab and delete/restore the infected files under the "Quarantine" tab.
   o Delete infected files automatically: Infected files will be deleted and cannot be recovered.

- o To receive an alert email when an infected file is found or after scanning has completed, configure the SMTP server settings in "System Settings" > "Notification" > "SMTP Server".

7. The scan job will run according to its schedule.

Button	Name	Description
▶	Run	Run the scan job now.
■	Stop	Stop the scan job.
✎	Edit	Edit the scan job settings.
🔍	View last run log	Open the last virus scan summary.
✖	Delete	Delete the scan job.

Reports

View or download the reports of the latest scan jobs on the NAS.

Button	Name	Description
⬇	Download	Download the virus scan report. The file can be opened by any text editor.
✖	Delete	Delete an entry on the list.
DOWNLOAD	Download All	Download all the virus scan logs on the list as a zip file.

Report options
- Specify the number of days (1-999) to retain the logs
- Enable the option "Archive logs after expiration" and specify the shared folder to save the logs to once the retention period has been reached. Click "Apply All" to save the changes.

Quarantine

This page shows the quarantined files on the NAS. Users can manually delete or restore quarantined files, or restore and add the files to the exclude list.

Button	Name	Description
✖	Delete	Delete an infected file. The file cannot be recovered.
↩	Restore	Restore an infected file to its original shared folder.
↩🔍	Exclude List	Restore an infected file and add the file into the exclude list (scan filter).
Restore Selected Files	Restore Selected Files	Restore multiple files on the list.
Delete Selected Files	Delete Selected Files	Delete multiple files on the list. The files cannot be recovered.
Delete All Files	Delete All Files	Delete all of the files on the list. The files cannot be recovered.

Backup Station

Configure the NAS as a backup server, remote replication, cloud backup and external backup with the Backup Station.
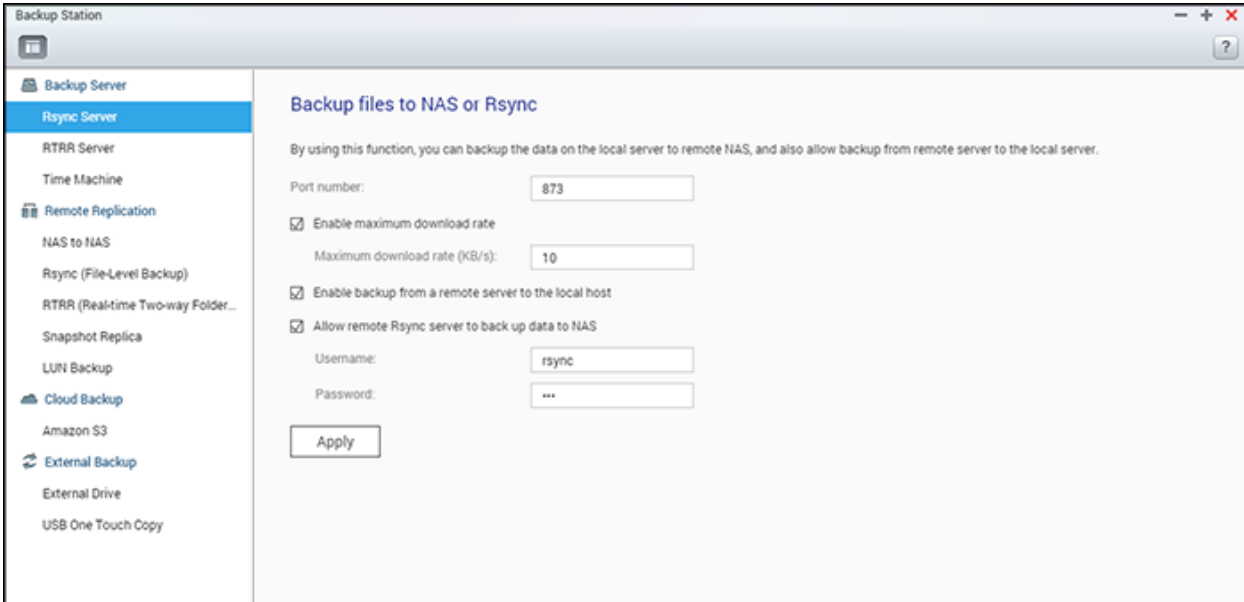
For details on the features, please refer to the following links:

- Backup Server
- Remote Replication
- Snapshot Replica
- Cloud Backup
- External Backup

> **Note:** Snapshots and related features are currently only available for the following NAS series: x51*, x53, x63, x70, x71, x79, x80.
> - * A minimum of 4 GB RAM is required to use snapshots.
> - * x51 series models only support up to 256 snapshots instead of 1024. The HS-251 does not support snapshots.

Backup Server

Rsync Server
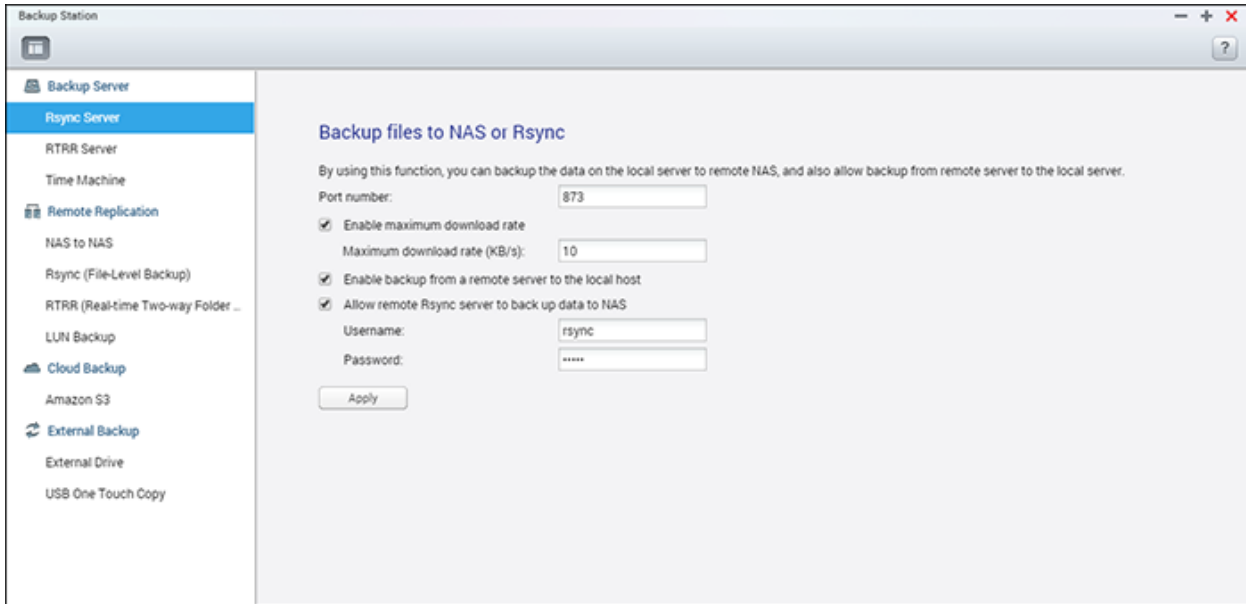
Enable Rsync server to configure the NAS as a backup server for data backup from a remote Rsync server or NAS server. The default port number for remote replication via Rsync is 873. Specify the maximum download rate for bandwidth control. 0 means unlimited.

- **Enable backup from a remote server to the local host:** Select this option to allow data backup from a remote server (NAS) to the local server (NAS).
- **Allow remote Rsync server to back up data to the NAS:** Select this option to allow data backup from an Rsync server to the local server (NAS). Enter the username and password to authenticate the Rsync server which attempts to back up data to the NAS.

> **Note:** You can only create up to 64 rsync jobs on the NAS.

RTRR Server
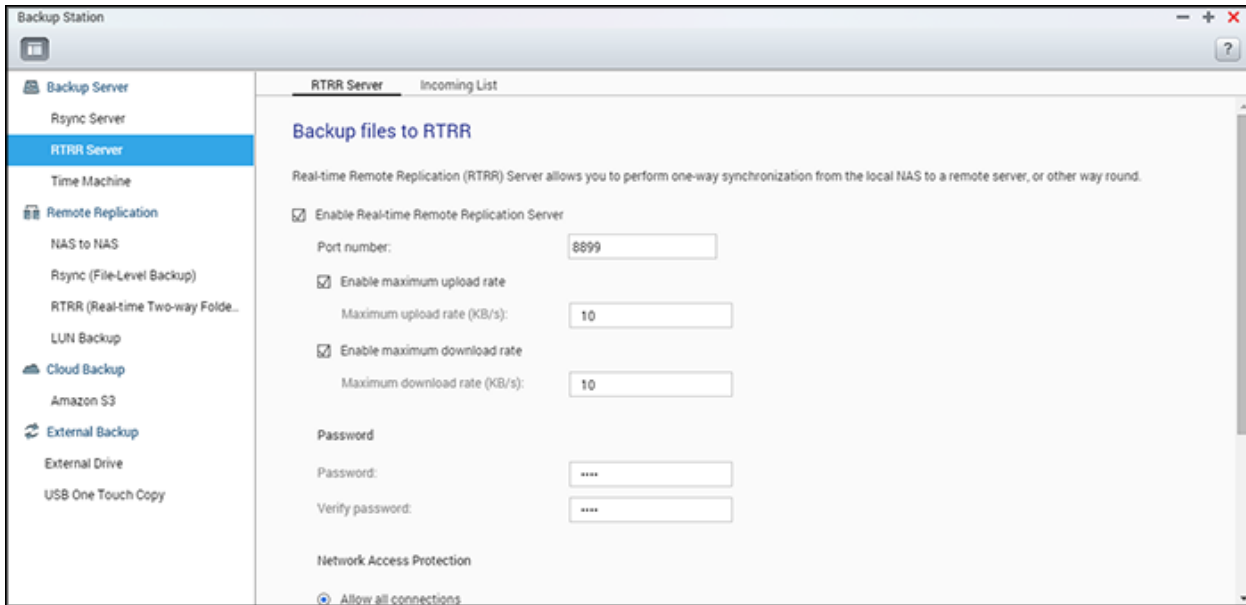
To allow real-time or schedule data replication from a remote server to a local NAS, select "Enable Real-time Remote Replication Server". You can specify the port number for remote replication. The default port number is 8899. Specify the maximum upload and download rate for bandwidth control. 0 means unlimited. To only allow authenticated access to back up data to the local NAS, specify the access password. The client server will be prompted to enter the password to back up data to the NAS via RTRR.

You can specify the IP addresses or host names which are allowed to access the NAS for remote replication. Up to 10 rules can be configured. To allow all connections, select "Allow all connections". To specify IP addresses or host names, select "Allow connections from the list only" and click "Add".

Enter an IP address or specify a range of IP addresses by entering the IP and subnet mask. Select the access right "Read Only" or "Read/Write". By selecting "Read/Write", the client server is allowed to delete files on the local NAS. Click "Finish" to exit. After saving the access rule, click "Apply" and the NAS will restart to apply the settings.

Check backup jobs from other NAS
You can check and manage backup jobs from other NAS that use the current NAS as a target destination for their backup. To check backup jobs, click the "Incoming List" tab and the details (including the job name, source NAS, destination NAS, job schedule and job status) of the backup jobs will be shown in the list. You can also manage backup jobs in this list. To do so, select backup jobs under "Incoming List" > choose to clear job records, open the backup folder, or deny access of the backup jobs to your NAS.

Time Machine

You can enable Time Machine support to use the NAS as a backup destination for Macs by the Time Machine feature on OS X.
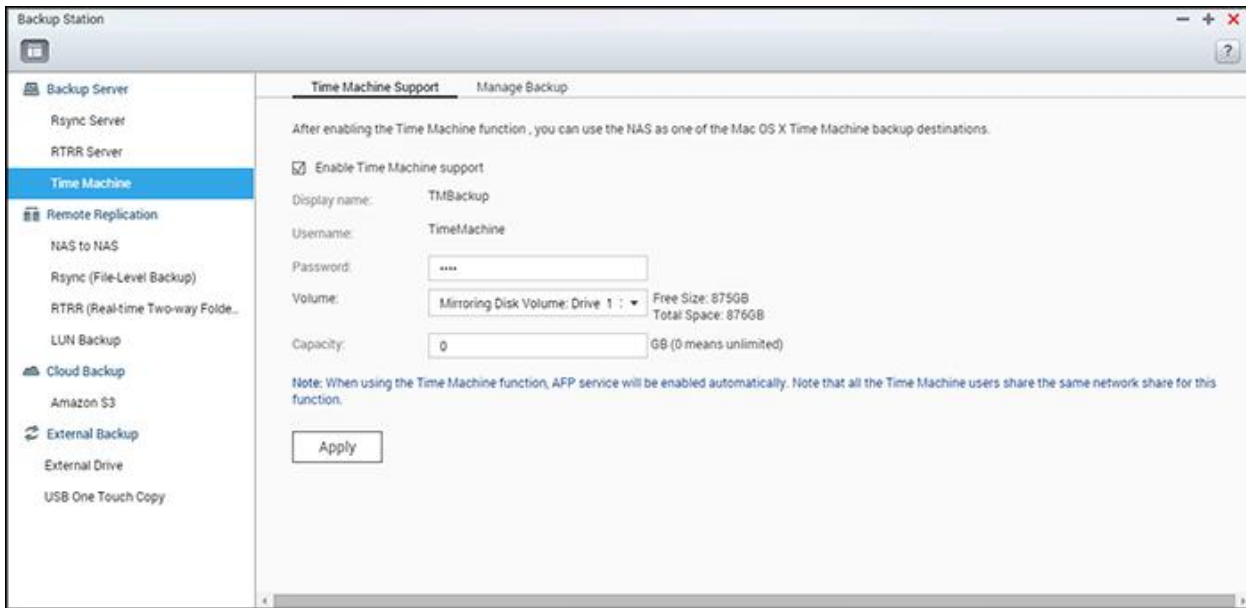
To use this function, follow these steps.

Configure the settings on the NAS:
1. Go to "Main Menu" > "Backup Station" > "Backup Server" > "Time Machine" > "Time Machine Support". Select "Enable Time Machine support".
2. Enter the Time Machine password. The password is empty by default.
3. Select a volume on the NAS as the backup destination.
4. Enter the storage capacity that Time Machine backup is allowed to use. The maximum value is 4095GB, 0 means unlimited.
5. Click "Apply" to save the settings.
6. Optional: Enable SMB 3.0 on Time Machine.
   Note: Mac OS Sierra is required.
   i. Go to "Control Panel" > "Win/Mac/NFS" > "Microsoft Networking" > "Advanced Options". The Advanced Options window will launch.
   ii. Select "SMB 3.0" in "Highest SMB version".

All the Time Machine users share the same shared folder for this function. Configure the backup settings on Mac:
1. Open Time Machine on your Mac and click "Select Backup Disk".
2. Select the TMBackup on your NAS from the list and click "Use for Backup".
3. Enter the username and password to login to the NAS and click "Connect".
   o Registered username: TimeMachine

o   Password: The password you have configured on the NAS. It is empty by default.
4. Upon successful connection, the Time Machine is switched "ON". The available space for backup is shown and the backup will start in 120 seconds.

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

Managing Backup

You can manage existing backups on this page.
- Volume (drop down menu on top right side of the screen): Display Time Machine backup tasks stored in the volume.
- Name: The name of the Time Machine backup (the sparse bundle disk image which was created by Time Machine.)
- Size: Size of this Time Machine backup.
- Date Modified: Last modified date of this Time Machine backup.
- Delete: Delete the selected Time Machine backup.

Remote Replication

This chapter covers the following topics:

- [NAS to NAS and Rsync](#)
- [RTRR](#)
- [Downloading Replication Job Logs](#)

Note: Starting from QTS 4.2, if a source storage pool supports snapshots, a snapshot will be taken before an Rsync or RTRR backup job starts to ensure data consistency. Please check that there is enough space reserved for taking snapshots before creating the job.

NAS to NAS and Rsync

The NAS data can be backed up to a remote NAS or Rsync server using Rsync remote replication.

For Rsync and NAS to NAS, there is no limitation for the maximum number of jobs. However, the actual result will be limited and affected by the size of NAS memory and the file structure. Each job supports 1 folder pair.
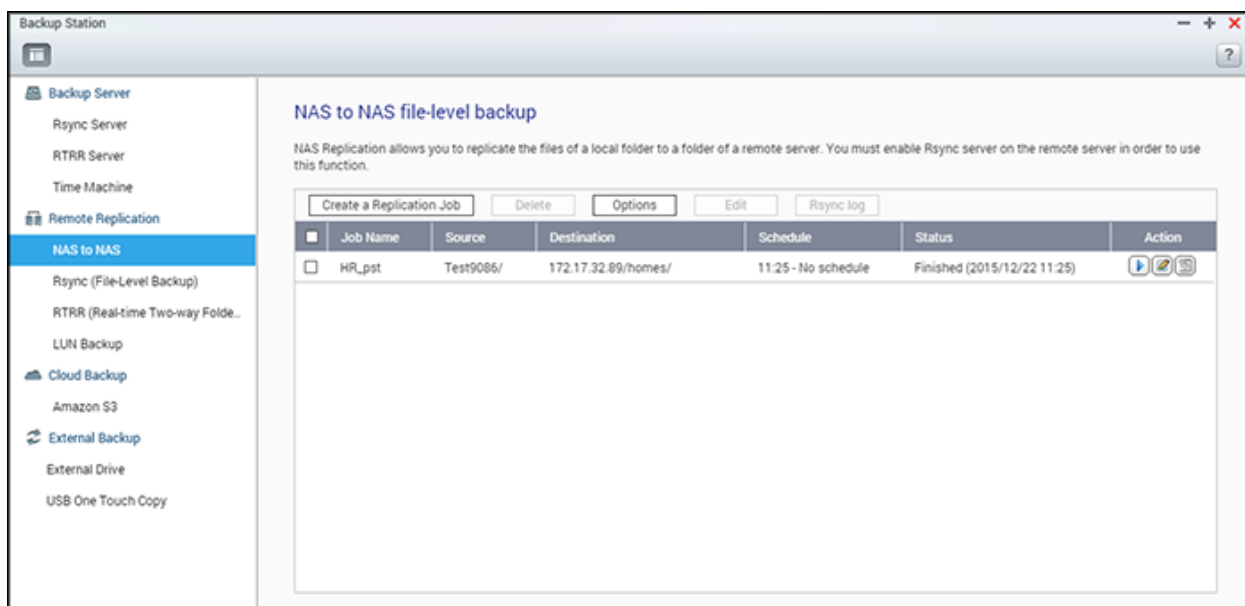
If the backup destination is a NAS, go to "Main Menu" > "Backup Station" > "Rsync Server" and enable the remote NAS as an Rsync backup server.

1. To create a replication job, click "Create a Replication Job".
2. Click "Settings".

3. Enter the IP address, port number, username and password to login to the remote server. The default port number is 873. The login username must have read/write access to the remote server and a sufficient quota limit on the server. Click "Test" to verify the connection, and then click "Apply".

4. Specify the local folder by clicking the Source folder box. After expanding and locating the folder, double click on it to set it as the directory where the data will be replicated from.

5. Specify the destination folder Destination folder box. Locate the folder in the folder tree and double click on it to set it as the directory where the data will be replicated to. And, click "Add" to add this pair of replication folders.

6. Click "Backup frequency" to configure the backup frequency. Select to immediately replicate the data or to specify a backup schedule.

7. Click "Options" and then select one of the following.

   o Enable encryption: Executes encrypted remote replication. Note that you must enable "Allow SSH connection" in "Network Services > "Telnet/SSH" and specify the same port number for SSH and encrypted remote replication.

   o Activate file compression: Allows file compression during the data transfer process. This option is recommended for low bandwidth environments or remote replication over WAN.

   o Only copy files that differ from files at the destination: Reduces the time required for transfers and minimizes the network traffic.

   o Delete extra files on remote destination: Synchronizes the source data with the destination data (one-way synchronization.) Extra files on the destination will be deleted. Source data remains unchanged.

   o Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turning on this option may reduce the time required for remote replication.

   o Replicate ACL and extended attributes: Keeps the information in extended attributes. Please note that the destination host needs to enable the same ACL functions or join to the same domain.

   o Enable maximum transfer rate: Specifies the maximum transfer rate.

8. Click "Apply". If you selected "Execute backup immediately", the replication task will start at once. Otherwise it will be performed 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.

Note: For step 5, the order of selecting the source and destination folders can be changed. The above is just an example.

Icon	Name	Description
	Start	Start a replication job immediately.

■	Stop	Stop a running replication job.
🔍	View	View Rsync logs (replication results).
✏️	Edit	Edit a replication job.
🚫	Disable	Disable replication schedule.
🕐	Enable	Enable replication schedule.

To configure the timeout and retry settings of the replications jobs, click "Options".

- Timeout (second): Specify a timeout value for each replication job. This is the maximum number of seconds to wait until a replication job is cancelled if no data has been received.
- Number of retries: Specify the number of times the NAS should try to execute a replication job if it fails.
- Retry intervals (second): Specify the number of seconds to wait in between each retry.

For example, if you entered 600 seconds for timeout, 3 retries, and 60 seconds for retry intervals, a replication job will timeout in 600 seconds if no data is received. The NAS will wait for 60 seconds and try to execute the job a second time. If the job timed out again, the NAS wait for another 60 seconds and retry for a third and final time.

RTRR
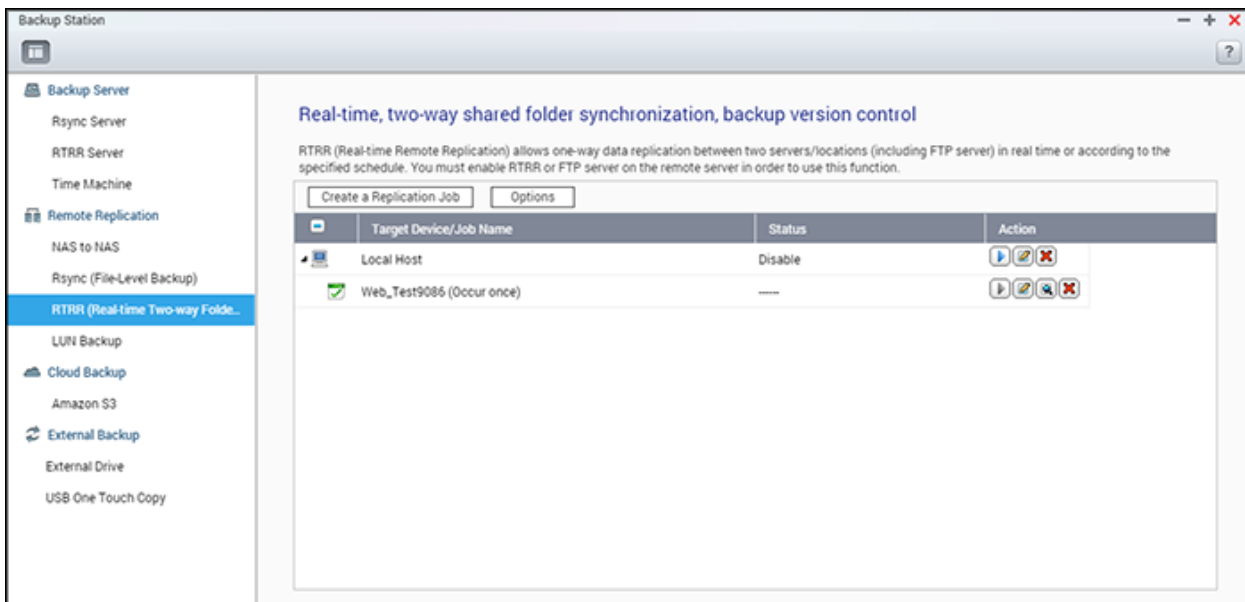
Real-time Remote Replication (RTRR) provides real-time or scheduled data replication and one-way and two-way data synchronization between two locations (such as a local NAS and a remote NAS, local NAS and an FTP server, or local NAS and an external drive, or replication between two local folders.) In real-time mode, the source folder will be monitored and any files that are new, changed, and renamed will be immediately replicated to the target folder. In scheduled mode, the source folder will be replicated to the target folder according to the pre-defined schedule.

One way synchronization refers to data synchronization from the source to the destination, while two-way synchronization means both the source and destination are synchronized after new files are copied in either side or files stored on either side are changed or deleted.

If the backup destination is a NAS, the RTRR server ("Main Menu" > "Backup Station" > "RTRR Server") or FTP service must first be enabled ("Main Menu" > "Control Panel" > "Network Services" > "FTP") on the remote NAS.

For RTRR, the maximum number of jobs is 400. Each job supports up to 16 folder pairs.

Follow these steps to create a replication job.
1. Click "Create a Replication Job".
2. When the wizard shows up, click "Next".
3. Select the synchronization locations and click "Next". Make sure the destination device has been formatted and folders have been created. Select the action to take (Backup, Synchronize, or Restore), the synchronization locations, and click "Next". Make sure the destination device has been formatted and folders have been created. For comparison between available actions and their folder pairs, refer to the following table:

Direction Action	Local folder to remote folder	Local folder to local folder/external drive	Remote folder to local folder
Backup	✔	✔	
Synchronization	✔	✔	✔
Restoration		✔	✔

Two synchronization options are available: one-way synchronization and two-way synchronization.
  o For one-way synchronization, you can choose to:
    ▪ Synchronize data from a local folder to a remote folder (NAS or FTP server)
    ▪ Synchronize data from a remote folder (NAS or FTP server) to a local folder
    ▪ Synchronize data from a local folder to another local folder or an external drive
  o For two-way synchronization, you can choose to:

- Synchronize data between the source and destination

4. Enter the IP address or host name. Select the server type (Windows Share (CIFS/SMB), FTP server or NAS server with RTRR service enabled; For two-way synchronization, only the NAS server is available.)

   o **Remote replication to FTP server:** Specify the port number and if you want to enable FTP with SSL/TLS (Explicit) for encrypted data transfer. If the FTP server is behind a firewall, enable passive mode. Enter the username and password with read/write access to the server. Click "Next".

   o **Remote replication to NAS with RTRR service:** Enter the IP address of the RTRR service-enabled server. Specify the connection port and select whether or not to enable secure connection. The default port number for remote replication via RTRR is 8899. Enter the password for RTRR connection. Click "Next".

   o **Remote replication to Windows Share (CIFS/SMB):** Enter the IP address of the Windows server. Specify the destination folder, username and password and click "Next".

5. Select the folder pair for data synchronization.

6. Each sync job supports up to 5 folder pairs. Select more folder pairs and click "Add". Click "Next".

7. Choose between real-time and scheduled synchronization. Real-time synchronization copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup. Scheduled synchronization copies files from the source folder to the target folder according to the pre-configured schedule. The options are:

   o Replicate Now: Replicate data immediately.

   o Periodically: Enter the time interval in hours and minutes that the backup should be executed. The minimum time interval is 5 minutes.

   o Hourly: Specify the minute when an hourly backup should be executed (for example, enter "01" to execute backup on the first minute of every hour.)

   o Daily: Specify the time when a daily backup should be executed (for example: 02:02 every day.)

   o Weekly: Select a day of the week and the time when a weekly backup should be executed.

   o Monthly: Select a day of the month and the time when a monthly backup should be executed.

   o Occurs once at: Specify the date and time the scheduled replication job will once be executed and this replication job will be executed only once.

Note:

- If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a replication job, you cannot select the folder as the source or destination of another folder pair of the same job.

- You can also create a folder as you select the folder pair. To do so, enter the folder name and click the folder icon from the drop down list.

- From QTS 4.1, RTRR can also back up the entire FTP site. To do so, select the root (/) from the

8. To configure synchronization policy, select "Configure policy and filter" and click "Next". Select whether or not to enable the following options:
   - Delete extra files: Delete extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time synchronization.
   - Detect sparse files: Select this option to ignore files of null data.
   - Check file contents: Specify to examine file contents, date, size, and name to determine if two files are identical. This option is not available for real-time synchronization.
   - Compress files during transmissions: Specify whether or not the files should be compressed for synchronization operations. Note that more CPU resources will be used.
   - Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.
   - Replicate ACL and extended attributes: Select this option to keep the information in extended attributes. Please note that the destination host needs to enable the same ACL functions or join to the same domain.
   - Filter system-generated temporary files: Filters temporary files created by system (including thumbnails and @recycle) will be filtered.
   - Timeout and retry settings: Specify the timeout period and retry settings if a synchronization operation fails.
9. Specify the file size, file types to include/exclude, and file date/time to filter data synchronization. Enter a job name.
   - File size: Specify the minimum and maximum size of the files to be replicated.
   - Last modified: Specify the number of days files are last modified for replication.
   - Include file types: Specify the file types to be replicated.
   - Exclude file types: Specify the file types to be excluded for replication.
   - File date/time: Specify the date and time of the files to be replicated.
10.   Click "Next".
11.   Confirm the settings and click "Next".
12.   Click "Finish" to exit the wizard.

Icon	Name	Description
▶	Enable and Start	Enable connection to a remote server. Start a replication job.
❚❚	Stop	Stop connection to a remote server or external drive.

■	Stop	Stop a replication job.
🔍	View	View job status and logs; download logs.
✎	Edit	Edit the connection settings of a remote server. Edit the settings of a replication job.
✖	Delete	Delete connection settings to a remote server. Delete a replication job. This button is available only after a replication job is stopped or the connection to the remote server is stopped.

To edit the replication job properties, click "Options".

Under "Event Logs" you can enable "Download Detailed Logs" and specify the maximum file size of log files. You can also set up sending email alerts when synchronization fails or completes. SMTP server settings must be set up on the NAS before using email alerts ("System Settings" > "Notification".)

Specify the replication policy in "Policy" and filter settings in "Filter". These will become the default settings for all RTRR replication jobs.

Downloading Replication Job Logs

To view the status and logs of a replication job, click the "View" button under "Action". You can view job logs or download them by clicking "Download Logs". Log files can be opened by Microsoft Excel or text editors. This button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed at least one replication job.

Snapshot Replica

The Snapshot Replica allows you to replicate the volume/LUNs between different remote servers using snapshot technology, which provides a flexible and efficient backup service for IT professionals.
To use this function, please enable the SSH server ("Control Panel" > "Network Services" > "Telnet/SSH") on the remote NAS first. Note that you may also access this function via Storage Manager ("Storage Manager" > "Storage Space"> "Snapshot" > "Snapshot Replica" for volumes or "Storage Manager" > "iSCSI Storage"> "Snapshot" > "Snapshot Replica" for LUNs.)

> **Note:** Snapshots and related features are currently only available for the following NAS series: x51*, x53, x63, x70, x71, x79, x80.
> - * A minimum of 4 GB RAM is required to use snapshots.
> - * x51 series models only support up to 256 snapshots instead of 1024. The HS-251 does not support snapshots.

Creating Replication Jobs

Follow these steps to create a snapshot replication job.
1. Click "Create a Replication Job".
2. Enter a name for this job.
3. Click "Settings" to specify the settings for the remote server. Enter the IP address, username and password for the remote server. Check "Local site" if the replication job is for your local NAS. Note that the login account must have read/write access to the remote server and sufficient quota limit on the server. Click "Test" to verify the connection. Then click "OK".
4. Select the local volume to take snapshot of by clicking the "Source Volume/LUN" drop-down list.
5. Select the destination pool to store the snapshots in the "Destination Pools" box.
6. Keep Snapshots: The maximum number is 1024. The system keeps this fixed number of versions and automatically rotates stored versions.
7. Click "Backup frequency" to configure the backup frequency. Select to replicate the data immediately or specify the backup schedule.
8. Specify other options as follows for the remote replication job by clicking the "Options" button and click "OK" after setup.
   - Enable encryption: Select this option to execute encrypted remote replication. Note that you must enable "Allow SSH connection" in "Network Services > "Telnet/SSH" and specify the same port number for SSH and encrypted remote replication.
   - Enable maximum transfer rate: Enter the value to restrict maximum available bandwidth in KB/s. If it is not specified, the bandwidth for this job is not limited.

- o Compress files during transmission: Enable this option to allow file compression during the data transfer process. This option is recommended for a low bandwidth environments or remote replication over WAN.
- o Replicate all snapshots: Select this option to replicate all snapshots. If this option is not selected, the system will only replicate the snapshot taken by the job.
9. Click "OK". If you select the "Execute backup immediately" option, the replication task will start at once. Otherwise, it will be performed according to your schedule. Note that the job is recursive. Do not turn off the local NAS and the remote server when remote replication is running.

Icon	Name	Description
▶	Enable and Start	Enable connection to a remote server. Start a replication job.
■	Stop	Stop a replication job.
🔍	View	View job status and logs; clear logs.
✎	Edit	Edit the settings of a replication job.
🕐	Enable/Disable Schedule	Enable or disable a scheduled replication job.

The system displays logs of all replications jobs at the bottom of the screen. Click "Clear all logs" to clear job logs.

Deleting Replication Jobs

1. Select a replication job from the list.
2. Click "Delete".
3. Click "OK".

Options

To change connection options, click "Options" and specify the timeout period of the number of connection retries.

In case the password used for access to the remote server is changed, you can click "Change Password" and click the "edit" button under "Action" to change the password used for that server.

To delete previous Snapshot Replica logs, click "Clear all logs".

Cloud Backup

Amazon S3

Amazon S3 (Simple Storage Service) is an online storage web service offered by AWS (Amazon Web Services.) It provides a simple web service interface that can be used to store and retrieve data from anywhere on the web. With Amazon S3, you can upload data from your NAS to Amazon S3 or download the data from Amazon S3 to your NAS. You need to register an AWS account from http://aws.amazon.com and pay for the service. After signing up, you need to create at least one bucket (root folder) on Amazon S3 using an Amazon S3 application. We recommend the Mozilla Firefox add-on "S3Fox" for beginners.
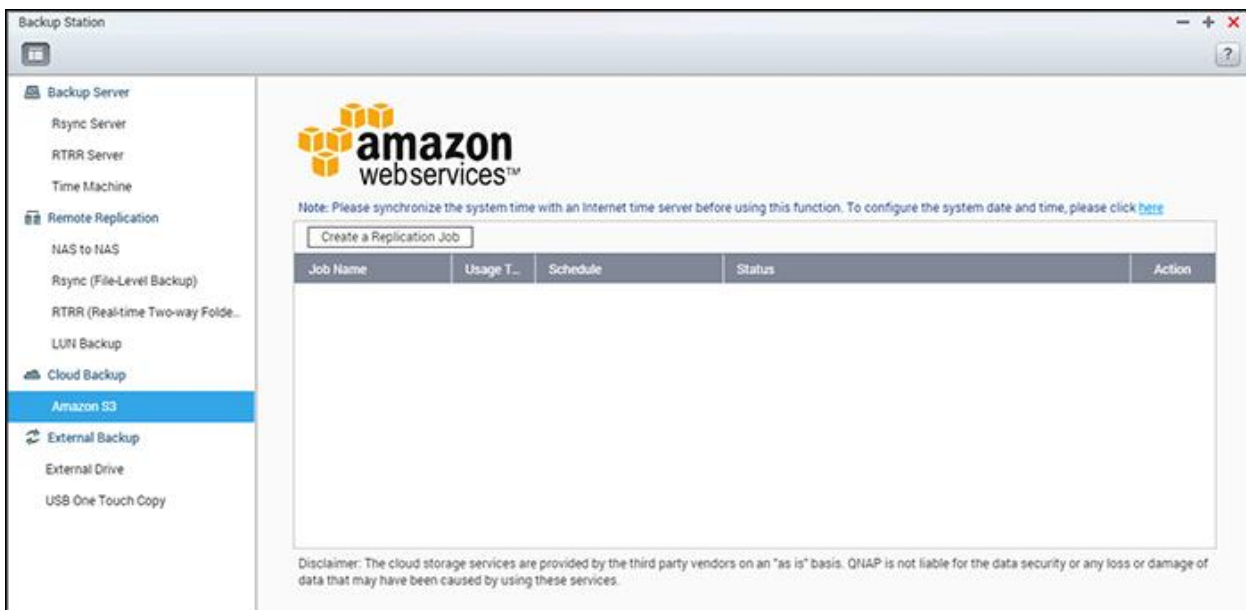
After setting up the Amazon S3 account, follow these steps to back up or retrieve data from Amazon S3 using the NAS.
1. Click "Create a Replication Job".
2. Enter the remote replication job name.
3. Select the usage type: "Upload" or "Download" and enter other settings. A bucket is the root directory on Amazon S3. You can test the connection to the remote host testing by clicking "Test". Other settings are optional.
4. Specify the local directory on the NAS for replication.
5. Enter the replication schedule.
6. Click "Finish". The replication job will be executed according to your schedule.
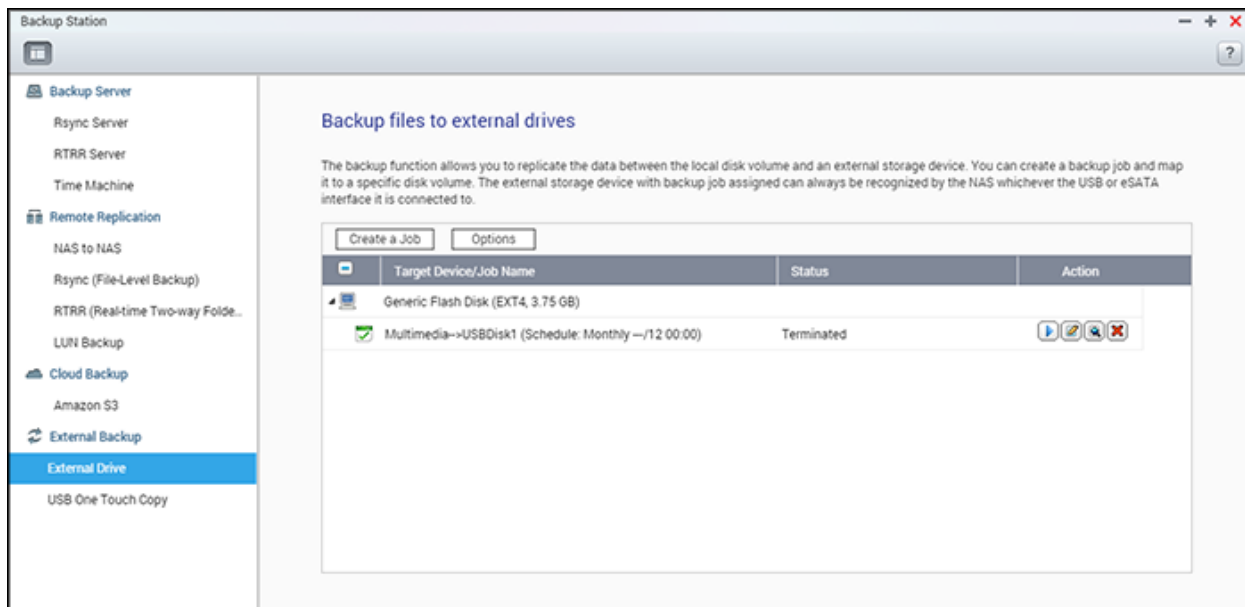
External Backup

The following topics are covered in this chapter:

- External Drive
- USB One Touch Copy

External Drive

The NAS supports real-time and scheduled data backup between internal disks volumes on the NAS and external USB/eSATA storage devices.

To use this feature, follow these steps.

> **Note:** If an external storage device is encrypted by the NAS, make sure it is unlocked in "External Device" > "External Storage" before creating any backup jobs.

1. Connect one or more storage devices to the USB or eSATA (if available) interfaces of the NAS.
2. Click "Create a new job".
3. When the wizard is shown, read the instructions carefully and click "Next".
4. Select the backup locations.
   a. Select an external disk volume from the drop-down menu. The NAS supports EXT3, EXT4, FAT, NTFS, and HFS+. The storage device's general information will be shown.
   b. Select "Map this backup job to the volume ID only" to map the backup job to this particular external storage device. The NAS will recognize the device and automatically

execute the backup job according to the settings every time it is connected to the NAS via any USB/eSATA interface.

    c. Select to back up the data from a local disk volume to the external storage or vice versa.

    d. Click "Next".

5. Select the source and destination folders for backup. Then click "Add". Up to 128 folder pairs can be created. Click "Next".

> **Note:**
> - Multiple partitions on the external storage device will be recognized as individual disk volumes.
> - If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a backup job, the same folder cannot be selected as the source or destination of another folder pair of the same backup job.
> - External Drive supports up to 100 jobs and each job supports up to 16 folder pairs.

6. Choose between real-time and scheduled backup. Real-time backup copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup. Scheduled backup copies files from the source folder to the target folder according to the schedule. The options are:

    o Replicate Now: Copy the data immediately.

    o Periodically: Enter the time interval in hours and minutes that the backup job should be executed. The minimum time interval is 5 minutes.

    o Hourly: Specify the minute when an hourly backup should be executed (for example, enter "01" to execute backup on the first minute of every hour).

    o Daily: Specify the time when a daily backup should be executed (for example: 02:02 every day).

    o Weekly: Select a day of the week and the time when a weekly backup should be executed.

    o Monthly: Select a day of the month and the time when a monthly backup should be executed.

    o Auto-Backup: Execute data backup automatically every time the device is connected and detected by the NAS.

7. Choose to automatically eject the external drive after the job is finished.

8. To configure the backup policy and filter settings, select "Configure policy and filter" and click "Next". Select whether or not to enable the following options:

    o Delete extra files: Deletes extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time data backup.

- o Detect sparse files: Select this option to ignore files with null data.
- o Overwrite the file if the source file is newer or the file size is different ·
- o Check file contents: Examine the file contents, date, size, and name to determine if two files are identical. This option is not available for real-time data backup.
- o Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.
9. Create filters for the backup job.
    - o File size: Specify the minimum and maximum sizes of the files to be copied.
    - o File date/time: Specify the date and time of the files to be copied.
    - o Include file types: Specify the file types to be copied.
    - o Exclude file types: Specify the file types to be excluded from the data copy.
10.   Enter a name for the backup job. A job name supports up to 63 characters and cannot start or end with a space.
11.   Confirm the settings and click "Next".
12.   Click "Finish" to exit the wizard.
13.   The backup job and the status will be shown on the list.

Button	Name	Description
	Start	Start a backup job.
	Stop	Stop a backup job.
	Edit	Edit the backup job.
	View / Download	View the job status and logs. Download the backup job logs.
	Delete	Delete a backup job. This button is only available after a backup job is stopped.

To disable a backup job's schedule, click "Edit" and select "Disabled" under "Settings" > "Schedule Type" and click "OK".

Default Backup Job Settings
1. To edit the default backup job properties, click "Options".
2. Under "Event Logs" you can select to enable "Download Detailed Logs" and specify the maximum file size of the log file. Select to send an email alert when a backup job fails or completes. Note that the SMTP server settings must be properly set up in "System Settings" > "Notification".
3. Specify the backup policy in "Policy" and filter settings in "Filter". These will become the default settings for all the backup jobs.

Download Backup Logs

1. To download a backup job's logs, make sure the option "Download Detailed Logs" is enabled in "Options" > "Event Logs".
2. Click the "View / Download" button in "Action" column of a backup job.
3. Go to "Job Logs" and click "Download Logs". The log file can be opened by Microsoft Excel or any text editor. This button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed a backup job.

USB One Touch Copy

Enable the USB one touch copy button to back up data from USB storage connected to the front-panel USB port to the NAS or vice versa.
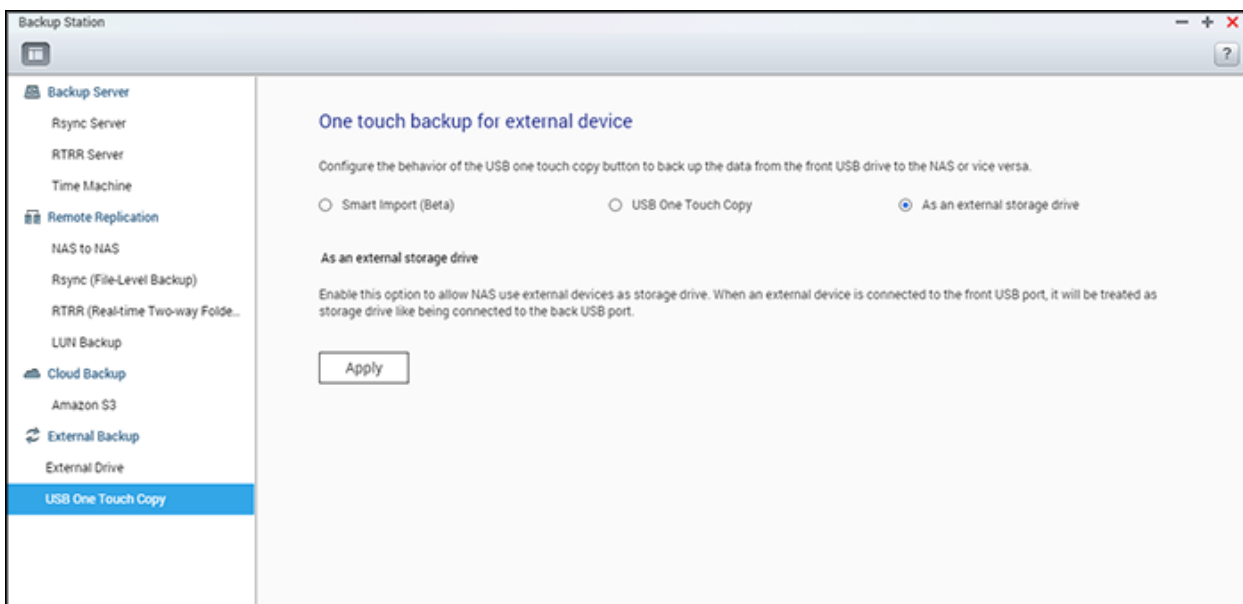
This feature is not supported by the TS-809U-RP, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, and TS-EC1279U-RP.

Smart Import (Beta)
When a USB device (such as a camera) is connected to the front USB port, all of the photos and videos on the device will be automatically imported to the NAS without pressing the "Copy" button. Imported files will be stored in "SmartImport," a newly-created folder, under the default backup directory. During each import, only new photos and videos will be imported to a new folder.

USB One Touch Copy
For customized backup configuration, please select "USB One Touch Copy."
- Backup direction: From the front USB drive to the NAS or vice versa.

- Backup method:
  - Create directory: A new directory will be created on the destination and the source data will be copied to this directory. The new directory will be named as the backup date (YYYYMMDD). If there are two or more backups on the same day, the directory will be named with YYYYMMDD-1, YYYYMMDD-2... and so on.
  - Copy: Back up data to the destination share. If the same file exists, the destination file will be overwritten.
  - Synchronize: Back up data to the destination share and clear the redundant files. If the same file exists, the destination file will be overwritten.
- Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turn on this option may reduce the time required for backup.
- Source and destination folders: Specify the folder pairs for backup and click "Add". Maximum 9 folder pairs can be added.
- Options: Click "Options" to set up notification of the backup jobs by email, SMS, or instant messaging (IM).
- Unmount the front USB drive manually: When enabled, users can press the Copy button for about 8–10 seconds until the USB LED light turns off and remove the front USB drive from the NAS.
- Enable the alarm buzzer:
  - One short beep: Backup has started.
  - Two short beeps: The front USB drive is being unmounted.

> **Note:** If there are multiple partitions on the source storage device, a new folder will be created for each partition on the destination as the backup folder. The backup folder will be named with the backup date and the partition number (YYYYMMDD-1 for partition 1, YYYYMMDD-2 for partition 2, etc). If the source storage device only contains one partition, the backup folder will be named YYYYMMDD.

Data copy using front USB port

The NAS supports instant data copy backup from USB devices to the NAS or vice versa using the one touch copy button. To use this function, follow these steps:

1. Make sure a hard drive is installed and formatted on the NAS.
2. Configure the behavior of the Copy button in "Backup Station" > "USB One Touch Copy".
3. Connect the USB device to the front USB port of the NAS.
4. Press the Copy button once. The data will be copied according to your settings.

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

> *Caution:* Files are copied from the source to the destination. **Extra files in the destination will be deleted. Files with the same names will be overwritten by the source.** Source data will remain unchanged.

As an external storage drive

When an external device is connected to the front USB port, it will be identified as an external storage drive connected to the port.

File Station

File Station is an online file management center. With the File Station, you can access the NAS across the Internet, manage files using a web browser, quickly find files, play media files, set file and folder permissions, and easily share your files and folders on the NAS.
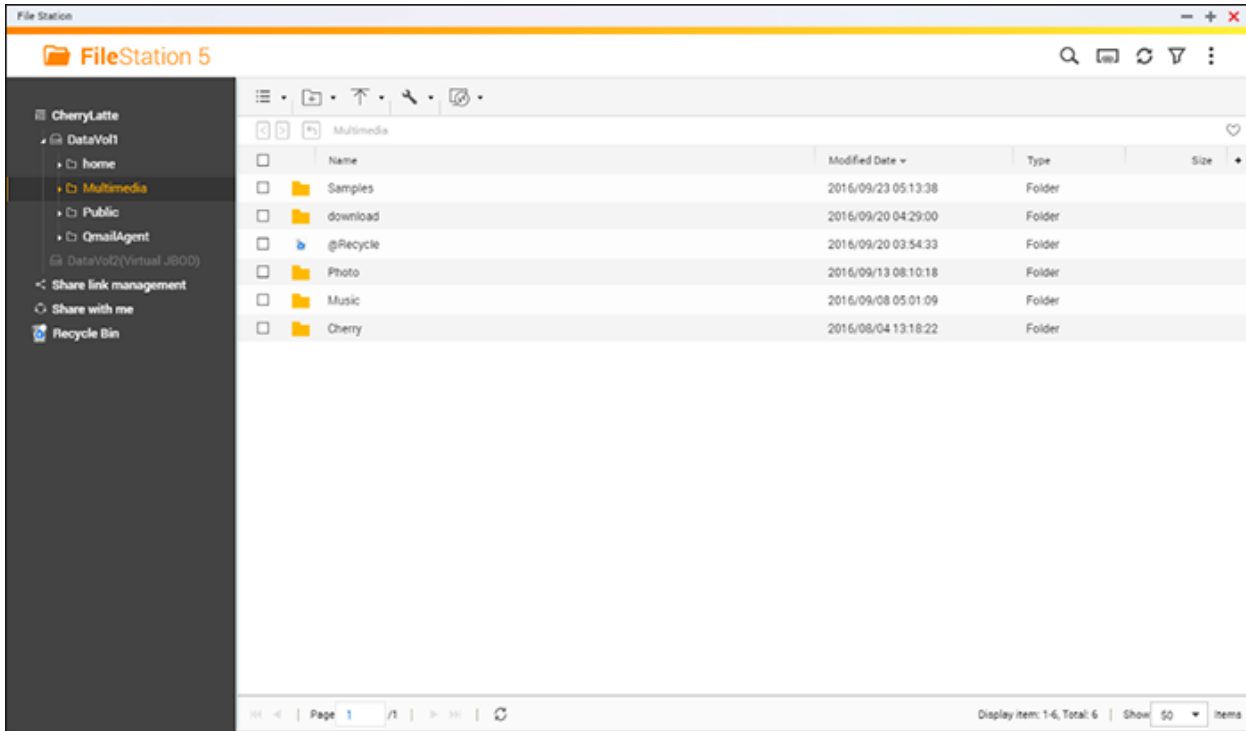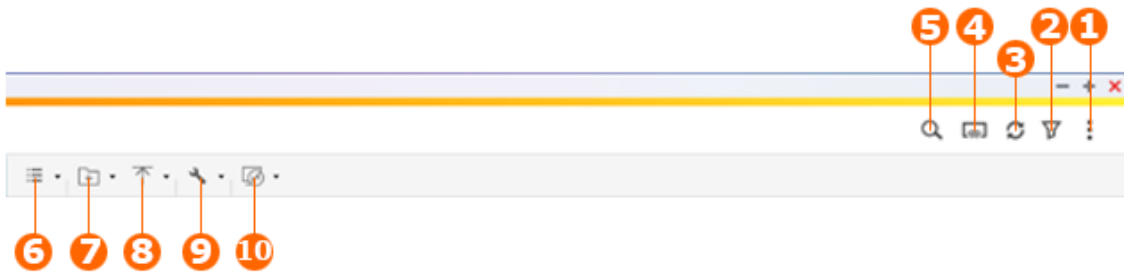

Topics covered in this chapter:

- Starting File Station
- Familiarizing yourself with File Station
- Using File Station
- Remote Mount

Starting File Station

Launch File Station from the Main Menu/Desktop shortcut, or directly log into File Station by going to: http://NAS_Name_or_IP/cgi-bin/filemanager.html.

Familiarizing yourself with File Station

Menu Bar

No.	Name	Description
1	Search	Search files by their name, file type (music, video, or photo) or with advanced search.
2	Network Media Player	Stream videos, photos and music to compatible devices in different rooms over your home network.
3	Refresh	Refresh the current page.
4	Smart File Filter	Filter files based on conditions set by users and the conditions will apply to all folders.

5	More settings	Click to display the following:
		• Settings – Select any of the following, as required.
		  o Show files and folders of my PC: Set to show/hide files and folders on the local PC. This allows you to see the contents of your PC in File Station. This feature is currently only available in Windows and requires Java to be installed (you can download it from http://java.com).
		  o Show hidden files on NAS: Set to show/hide hidden files.
		  o Allow all users to create shared links.
		  o Support multimedia playback and thumbnail display: If this option is checked, the file icon will be displayed as thumbnails.
		  o Show Network Recycle Bin(s): Set to show/hide the "@Recycle" folder.
		  o Only allow the admin and administrators group to use "Share to NAS user".
		  o Only allow the admin and administrators group to permanently delete files: Check this option and 1)

		only administrators can permanently delete files from File Station; and 2) files deleted by other users will be moved to the Trash.
		○ Remote mount: Configure the groups of users (administrators, administrators group, or specific users) that are allowed to use the Remote Mount feature.
		• Help – Open the File Station Help.
		• About – Display information about File Station.
6	Browsing Mode	Select a browsing mode: • List • Large icons • Medium icons • Small icons
7	Create folder	Create a folder/shared folder or share space with a user (see the below Sharing NAS space section.)
8	Upload	Upload files or folders to the selected shared folder.
9	More Action	• Bookmark the selected shared folder (and it will appear under "Favorites" on the left panel). • Perform file or folder operations including open, download, rename, copy/move, delete, cut, create desktop shortcut, compress, transcode files/folders (these options are only available when files and/or folders are selected). • Check folder properties. • Review transcode information, background tasks (file compression, file upload and moving files within the NAS) or storage information.
10	Remote Mount	• Create remote mounts • Check connection records and the current connection status (see Remote Mount)

Tip: If you are using Google Chrome, you can drag and drop files from your PC to File Station. However, some computers may not be able to upload files that are larger than 1GB using this method due to their low performance. When this happens, please consider uploading using File Station.

Note:

- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your NAS does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, see Transcode Management.
- If your NAS supports transcoding, please install the CodexPack App before using this function. The NAS will try to transcode to a suitable format for your device. If your NAS does not support transcoding, the NAS will only output the original file format and the seek function may not work properly. In this case, please make sure that your device is compatible with the file format used by the video.
- Some video formats may experience issues when streaming via DLNA, Apple TV or Chromecast. If any of these issues arise during video playback, you can consider transcoding your videos into universally-compatible media formats. For more details on transcoding, please refer to the Transcode Management chapter.
- Some media players do not support pausing during playback. If this happens, playback will continue even if you use the pause feature.
- For multimedia files transcoded using on-the-fly Transcoding, the time displayed on the media player seek bar will become 00:00 while you forward or rewind the multimedia files during playback.
- The original photo files will be used for streaming if their thumbnails are not available.

Left Panel

- Volume: Every shared folder and folder on the NAS is listed here. Depending on your NAS model, the default shared folders are different and can include "Download", "homes", "Multimedia", "Public", "Recordings", "USB" and "Web". You can click "+" next to a volume to create a shared folder on the volume.
- Local folders: Folders on your local PC are listed here. The Java JRE must be installed to use this feature.
- Favorites: Bookmarked folders are listed here.
- Qsync: Folders or files synchronized from the Qsync service, and team folders are listed here.
- Share link management: Links of files shared from the NAS are listed here.
- Share with me: Files and folders that have been shared to you from other NAS users are listed here.
- Recycle Bin: Deleted files or folders can be found here. Right-click on deleted items in the recycle bin to permanently delete or recover them.

Using File Station

Creating shared folders

To create a shared folder, click "Create folder" and select "Shared folder". Specify the folder name, folder description, disk volume, user access privileges, and advanced settings in the shared folder creation dialog window and click "Create".

Subfolder operations

Right-click a subfolder and select one of the following actions:

Action	Description
Sort By	Sort all the subfolders and files within the page by name, modified date, type, or size.
Create folder	Create a subfolder.
Copy/Paste	Copy a subfolder and paste it into another shared folder.
Share	• Share the selected folder via email; • Publish the selected folder on social networks; • Set sharing details
Open	Enter the chosen subfolder.
Download	Compress and download the subfolder.
Rename	Rename the subfolder.
Copy to/Move to	Copy or move the subfolder to another location on the NAS.
Delete	Delete the subfolder.
Cut/Paste	Cut a subfolder and paste it to another shared folder.
Add to Transcode	Create transcode tasks for the files within the subfolder. If you see certain resolution options disabled in the "Add to Transcode" window, it means the selected video files have already been transcoded into these resolutions. **Note: This feature is for the x86 series NAS only.**
Cancel/Delete Transcoding	Cancel / Delete transcode tasks created for the subfolder
Transcode Information	Bring up the Transcode Task window for your review on transcode tasks.
Create Shortcut to Desktop	Create a shortcut icon on the Desktop for the selected folder.

Add to Favorites	Bookmark the subfolder and it will appear under "Favorites" in the left panel.
Compress(Zip)	Compress the subfolder.
Properties	Display the properties in a new window.

Tip: For folders and files, the shortcut keys are provided for quick file and folder operations. Available shortcut keys include:

- Ctrl + C: Copy selected files/folders.
- Ctrl + V: Paste selected files/folders.
- Ctrl + X: Cut selected files/folders.
- Ctrl + A: Select all files/folders.
- Del: Delete selected files/folders.
- F2: Rename the selected file/folder.
- F5: Reload the current list.

File operations

Right-click a file and select one of the following actions:

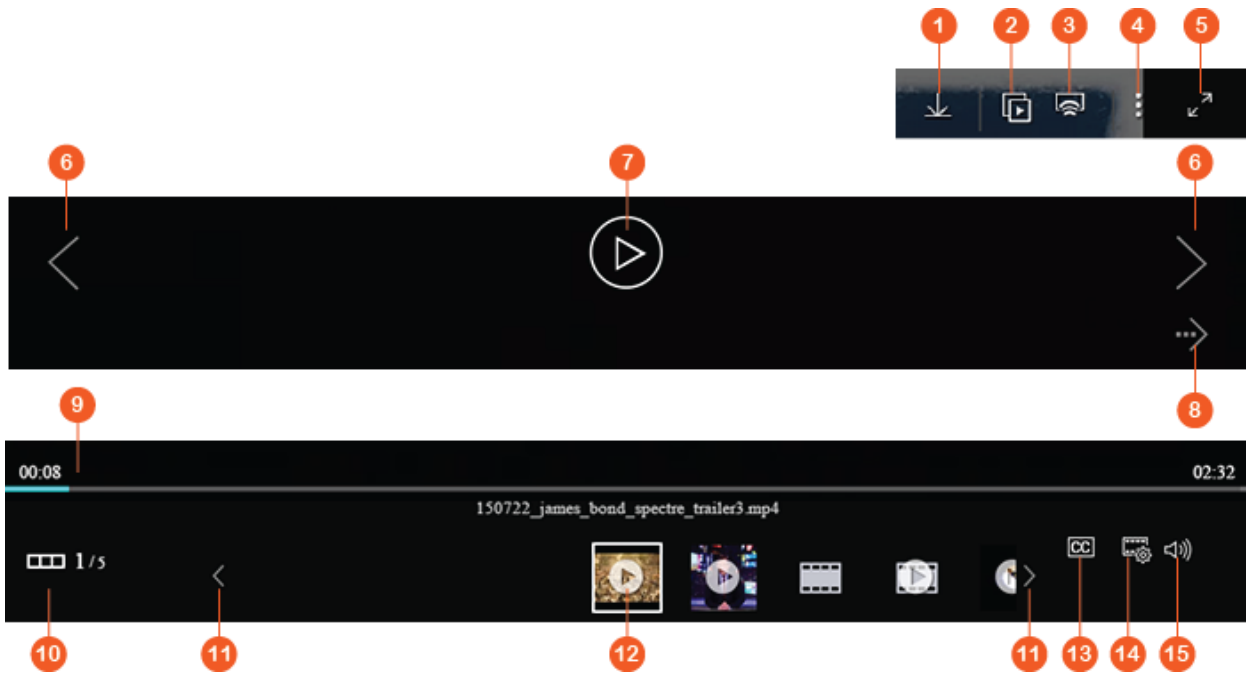| Action	Description
Sort By	Sort all the subfolders and files within the page by name, modified date, type, or size.
Copy/Paste	Copy a subfolder and paste it into another shared folder.
Share	Share selected files/folders via email, social network, by shared links, or to other NAS users. Refer to the Sharing files section for more details.
View in Office Online	Open Office files stored on the NAS using Office Online. The document will be first uploaded to Office Online and opened in a new browser tab. You must first install and sign in to the myQNAPcloud App to use this function.
View in Google Docs	Open Office files stored on the NAS using Google Docs. The document will be first uploaded to Office Online and opened in a new browser tab. You must first install and sign in to the myQNAPcloud App to use this function.
Open with Chrome Extension	Preview and edit Microsoft Office files offline with a Chrome browser extension (Chrome only and requires the "Office Editing for Docs, Sheets & Slides" Chrome extension to be installed.)

Streaming to (Network Media Player)	Stream multimedia files (videos, music, and photos) to compatible devices in different rooms over your home network.
Play	Launch the Media Viewer and play the selected item.
Open	Open the file with a corresponding application on your PC. If no such applications are available, the file will be downloaded instead.
Open with VLC	If the chosen file is a video file, it will be opened in the browser (the VLC plug-in needs to be installed first.)
Download	Download the file. If the chosen file is a video that has been transcoded, you can choose its resolution and download the file. If multiple files are selected for download, they will be compressed before the download.
Rename	Rename the file.
Copy to/Move to	Copy or move the file to another location on the NAS.
Delete	Delete the file.
Cut/Paste	Cut a file and paste it to another shared folder.
Add to Transcode	Create a transcode task for the file. Create transcode tasks for files within the subfolder. If you see certain resolution options disabled in the "Add to Transcode" window, it means the selected video files have already been transcoded into these resolutions. **Note: This feature is for the x86 series NAS only.**
Cancel/Delete Transcoding	Cancel/Delete transcode task.
Transcode Information	Bring up the Transcode Task window for you to review transcode tasks.
Extract	Extract the compressed file.
Compress(Zip)	Compress the file.
Mount ISO	Mount the iso image as a shared folder on the left panel. After the file is mounted, you can click that shared folder to access the content of that iso image. To unmount an iso file, right click on the iso-mounted shared folder in the left panel and choose "Unmount".
Properties	Display the properties in a new window.

Playing media files

To play media files with File Station, double-click a multimedia file (photo, music and video files) and the Media Viewer (a built-in media player on the NAS) plays the file. Use the following buttons to control the Media Viewer:

No	Name	Description
1	Download	Download the item.
2	Slideshow	Play all chosen photos as a slideshow. You can adjust the speed and effect of the slideshow (for photos only.)
3	Network Media Player	Stream videos to compatible devices in different rooms over your home network.
4	More Action	Rotate the photo, set the photo as the QTS wallpaper, or delete the photo/video.
5	Full Screen	Switch to full screen mode.
6	Previous Item/Next Item	Play the previous/next item.
7	Play/Pause (videos)	Play/Pause the video.
8	Play/Pause (photos)	Play/Pause photos as slideshow.
9	Seek Bar	Control the playback progress.
10	Show/Hide Preview Bar	Hide/show the preview bar.
11	Last Item/Next Item	Play the last/next item on the preview bar.
12	Preview Bar	Preview the items in queue.
13	Subtitle	Manage subtitles of the video.
14	Resolution	Change resolution and transcoding settings.

15	Volume	Adjust the volume.

Finding your files/folders quickly

File Station supports smart searching for files, sub-folders, and folders on the NAS. You can search for files or folders using all or part of the file/folder name, by file type, or by file extension. There are two additional approaches you can quickly find your files: 1) advanced search and 2) smart file filter.

- For the advanced search, first click the magnifier on the search bar and then select "Advanced Search". Specify the search conditions (including name, size, date files are modified, location, type and owner/group) and click "Search". The files that match these conditions in the current folder will be listed.
- For the smart file filter, click "Smart File Filter" in the Main Menu. Specify the filtering conditions (including name, size, date files are modified, type and owner/group) and click "OK". Files that match the conditions will be listed for the folder. This is the case even if you switch to a different folder.

Setting file/folder level permission

You can set file or folder level permissions on the NAS using File Station. Right-click on a file/folder and select "Properties".

If "Advanced Folder Permissions" is disabled in "Privilege Settings" > "Shared Folder" > "Advanced Permissions", the following settings will be shown. Define the Read, Write, and Execute access rights for Owner, Group, and Others.

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

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

If the "Enable Advanced Folder Permissions" option is enabled in "Privilege Settings" > "Shared Folder" > "Advanced Permissions", you will be able to specify the file and folder permissions by users and user groups. Click + to do so.

To select users and user groups and specify the Read and Write permissions, click "Add".

To remove permissions on the list, select the users or user groups and click "−".

You can also define the file and folder owner by clicking the edit button next to the owner field. To do this, select a user from the list or search for a username, and then, click "Set".

The following options are available for folder permission settings. It is recommended to configure folder permissions and subfolder permissions in "Privilege Settings" > "Shared Folders".

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

Sharing files

To share files on the NAS using File Station, right click on the files/folders and select "Share". There are four sharing methods:

- Via email: Enter the required fields (including mail server from NAS or local computer, sender, recipient, subject, message, domain name/IP and link name), choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Finally, preview the settings or directly share the file.

Note: To share files/folders using your own email account, your email account must be set up in QTS Desktop > "Options" > "E-mail Account".

- To social networks: Enter the required fields (including the social network to share the file, post message, domain name/IP and link name) choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings".

- Create share links only (generate a link to provide on instant messengers or store for later use): Complete required files (domain name/IP and link name), choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings".

- To NAS users: Choose to share with new or existing NAS users.
  - For new NAS users, fill out account details (username and password), choose to allocate the quote, choose whether to send an email notification (and fill out message subject and content), set domain name/IP, link name and password for the link, decide whether to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Click "Preview" to preview the message or "Share Now".
  - For existing users, select existing user account(s), choose whether to send a notification email to the user (and fill out message subject and content), set domain name/IP, link name and password for the link, decide whether to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Click "Preview" to preview the message or "Share Now".

For folders, there will be an option "Allow file upload to this folder" in the dialog window for all four sharing options. This feature is only for administrators and can allow link recipients to upload files to the folder pointed to by the link.

For the "To NAS users" option, if you choose to share with new NAS users, the system will create new user accounts. Also, the email recipients (or users you share files with) can check files shared in File Station > "Share with me" on the left panel after they log into the NAS.

Sharing NAS space

Administrators can allocate space to NAS users and specify a storage quota in File Station by following these steps:

1. Click "Create" (the "+" icon) on the Menu Bar > "Share space with a user".
2. Complete the required fields in the "Create a User" page.
3. Enable the quota feature and set the quota size in "Control Panel" > "Privilege Settings" > Quota" if you have not already done so.
4. Specify the email (optional) and phone number (optional) for the user.
5. Choose to send an email notification to the newly-created user (optional), fill out the message details (including mail server (from NAS or local computer), sender, recipient, subject, message, domain name/IP and link name) and choose to include SSL (https://) in the URL.
6. Click "Create".

Remote Mount

The remote connection mount service allows you to easily manage files across local devices, external devices, cloud services and remote devices from a single interface. You can easily carry out file management tasks such as copying and moving from remote to local devices or vice versa. The remote connection mount service supports multiple cloud services (such as Google Drive, Dropbox, and OneDrive), and remote device network protocols (such as CIFS/SMB, and FTP.), and automatic searches for local devices.

Create remote mounts
1. Click "Remote Mount" > "Create remote mount".
2. Choose to connect to a remote storage via Auto Search, SMB/CIFS, or FTP.
3. Fill out the necessary details (including the protocol, codepage, hostname/IP, port, username/password, destination folder, and connection name) and choose to enable support for multimedia playback and thumbnail display (the system will generate thumbnails at the destination. If the destination is another QNAP NAS, it must have QTS 4.2 or later installed).
4. Click "Create".

Check recent connection records
1. Click "Remote Mount" > "Connection record".
2. Review recent connection records and their details including the connection time, connection name, protocol, Hostname/IP, port, account username, codepage and source path.
3. To sort the records, click on a header.

Check the current connection status
1. Click "Remote Mount" > "Current connection status".
2. Review the status of the current connections records and their details, including the owner, connection time, protocol, Hostname/IP, port, source path, status and creation time.
3. To sort records, click on a header.
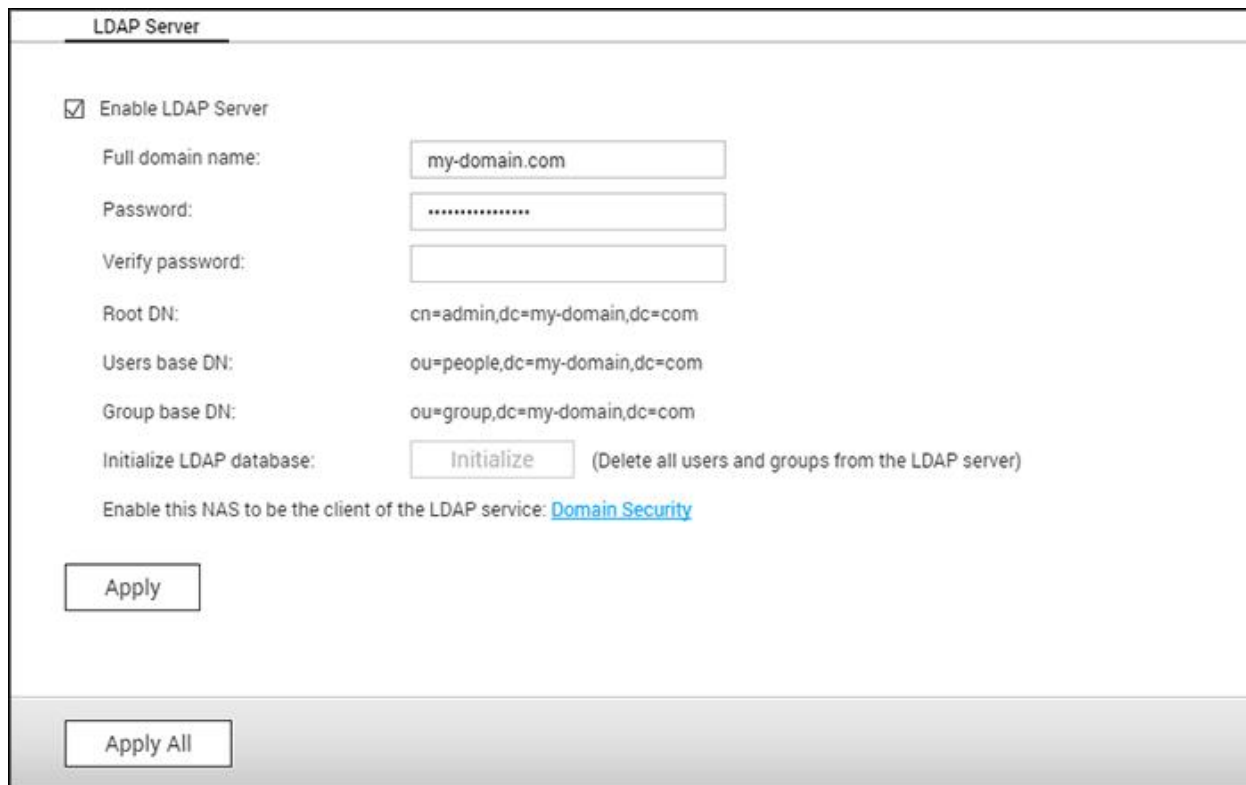
> **Notes:**
> - The maximum number of remote mounts that can be created per NAS is 256.
> - To share links by email, the email server settings must be properly configured in "System Settings" > "Notification" > "SMTP Server".
> - Up to 1000 sharing links are supported.
> - For best performance, use one of the following browsers: IE 9+, Firefox 3.6+, Safari 5+, or Chrome.

- Do not close the browser before the file transfer process (upload or download) is completed or the process will fail.
- To use Remote Mount, you must install the Connect to Cloud Drive app from the App Center before connecting to cloud services.
- Using a remote mount is identical to an external device and ongoing tasks will be terminated if the NAS is restarted or powered off.
- Limitations of your cloud service account may affect what files can be transferred. Please check the account details with your cloud service providers for more information regarding what files can and cannot be transferred.
- When transferring a large amount of files over CIFS/SMB using a remote mount, some antivirus software may cause the transfer to fail. If you encounter this problem, please temporarily disable your antivirus software and try again.
- Due to performance limitations of web browsers and PCs, you may not be able to upload a large amount of files in one task. If you encounter this problem, please separate your upload task into multiple tasks or use another upload method.

LDAP Server

The LDAP server of the NAS allows the administrator to create users to access multiple NAS servers with the same username and password.

Configuring LDAP Server

Follow these instructions to configure the LDAP server.

1. Enable LDAP Server: Log in to the NAS as "admin". Go to "Control Panel" > "Applications" > "LDAP Server" and enable the LDAP server. Enter the full LDAP domain name and the password for the LDAP server, then click "Apply".
2. Create LDAP Users: Under the "Users" tab, click "Create" then click "Create a User" or "Create Multiple Users" or "Batch Import Users". Follow the wizard instructions to create LDAP users. Once you have created the LDAP users, the NAS can be joined to the domain. You can set the permissions of LDAP users and allow them to be authenticated by the NAS.
3. Join a NAS to LDAP Domain: To allow LDAP users to connect to the NAS, join the NAS to the LDAP domain. Go to "Privilege" > "Domain Security". Select "LDAP authentication" and choose "LDAP server of local NAS" as the server type. Then click "Apply". The NAS is now a client of the LDAP server. To view the domain users or groups, go to "Privilege Settings" > "Users" or "User Groups", then select "Domain Users" or "Domain Groups". You can also set the folder permission for the domain users or groups.

4. Join a Second NAS to LDAP Domain: You can join multiple NAS to the same LDAP domain and allow the LDAP users to connect to these NAS using the same login credentials. To join another NAS to the LDAP domain, login to the NAS and go to "Privilege" > "Domain Security", select "LDAP authentication" and set "LDAP server of a remote NAS" as the server type. Enter the DNS name or IP address of the remote NAS, the name of the previously-created LDAP domain, and enter the LDAP server password. Click "Apply".

Backing up/Restoring LDAP Database

To back up the LDAP database on the NAS, select "Back up Database" and specify the backup frequency, destination folder on the NAS and other options. To restore an LDAP database, browse to select the *.exp file and click "Import".

> **Note:**
> - If the name of a user is changed in a LDAP server, it is necessary to assign the folder permissions again on the NAS.
> - To avoid account conflicts, do not create NAS local user accounts that already exist in the LDAP directory.

QVPN Service

The NAS supports Virtual Private Network (VPN) service for users to access the NAS and resources on a private network from the Internet. Use QVPN Service to set up your NAS as a VPN server and establish a VPN client connection.

In this chapter, the following topics are covered:

- VPN Server Setup

- Third Party VPN Client Setup and Connection

- Privilege Settings

- Connection List

- Connect a VPN Server via PPTP

- Connect a VPN Server via OpenVPN

- Connect a VPN Server via L2TP/IPSec

- Logs

VPN Server Setup

1. Enable PPTP, OpenVPN, or L2TP/IPSec: The NAS supports PPTP, OpenVPN or L2TP/IPSec for VPN connection. Select one of the following options and configure the settings.

o **PPTP**: Point-to-Point Tunneling Protocol (PPTP) is one of the most commonly used methods for VPN connection. It is natively supported by Windows, Mac, Linux, Android, and iPhone. You can also specify the VPN client IP pool and advanced settings (including the maximum number of clients, authentication protocol, encryption method, network interface and DNS server).

o **OpenVPN**: OpenVPN is an open source VPN solution which utilizes SSL encryption for secure connection. To connect to the OpenVPN server, the OpenVPN client must be installed on your PC. Click "Download Configuration File" to download the VPN client settings, certificate/key and installation guide from the NAS and upload the files to the OpenVPN client. You can also specify the VPN client IP pool and advanced settings (including the VPN server port, maximum number of clients, encryption method, network interface, DNS server, and whether to use the redirect-gateway and compressed data before their transfer via VPN).

o **L2TP/IPSec**: L2TP (Layer Two Tunneling Protocol) is a combination of the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F). Compared to PPTP, which only establishes a single tunnel between the two end points, L2TP supports the use of multiple tunnels. IPSec is often used to secure L2TP packets by providing confidentiality, authentication and integrity checks. The combination of these two protocols provides a high-security VPN solution which is known as L2TP/IPSec. L2TP/IPSec is supported by most clients, including Windows, Mac, Linux, and mobile devices.

2. Configure port forwarding by auto router configuration: The NAS supports auto port forwarding for UPnP (Universal Plug-and-Play network protocol) routers. Go to "myQNAPcloud" > "Auto Router Configuration" to enable UPnP port forwarding and open the ports of the PPTP, OpenVPN or L2TP/IPSec service on the router.

3. Register myQNAPcloud service: You can connect to the NAS by WAN IP or myQNAPcloud name. To configure myQNAPcloud service, check the chapter on myQNAPcloud Service or visit myQNAPcloud (https://www.myqnapcloud.com).

4. Add VPN users: Go to "QVPN Service" > "Privilege Settings", click "Add VPN Users". The local NAS users will be listed. Select the users who are allowed to use the VPN service and their connection method (PPTP, OpenVPN or L2TP/IPSec, multiple methods are also allowed). Click "Add".

5. Connect to the private network by a VPN client device: Now you can use your VPN client device to connect to the NAS via the VPN service.

Notes:

- The default NAS IP is 10.0.0.1 under PPTP VPN connection.
- Upload the configuration file to the OpenVPN client every time the OpenVPN settings, myQNAPcloud name, or the secure certificate is changed.
- To connect to the PPTP or L2TP/IPSec server on the Internet, the PPTP or L2TP/IPSec passthrough options on some routers have to be opened. PPTP uses only port TCP-1723 and L2TP/IPSec uses UDP 500, 1701 and 4500; forward those ports manually if your router does not support UPnP.

Third-Party VPN Client Setup and Connection

PPTP on Windows 8

1. Go to "Control Panel" > "Network and Sharing Center".

2. Select "Set up a new connection or network".

3. Select "Connect to a workplace" and click "Next".

4. Select "Use my Internet connection (VPN)".

5. Enter your myQNAPcloud name or IP address in "Internet address".

6. Enter a name for the connection in "Destination name".

7. Click "Create".

8. Go to "Control Panel" > "Network and Sharing Center" > "Change adapter settings".

9. Right-click the VPN connection and then select "Properties".

10.   Enter "Security" page, select the "Type of VPN" as PPTP.

11.   Click "OK".

PPTP on Mac OS X 10.10

1. Go to "Apple menu" > "System Preferences", and click "Network".

2. Click "Add (+)" at the bottom of the list, and choose "VPN" as the interface.

3. Select "Add new service (+)" and choose "VPN" in "Interface".

4. Select "PPTP" in "VPN Type".

5. Enter a name for the connection in "Service Name".

6. Enter your myQNAPcloud name or IP address in "Server Address" and your QNAP NAS user name in "Account Name".

7. Click " Authentication Settings" and then enter the password and preshared key.

8. Click "Connect".

PPTP on Android 5.0

1. Go to "Settings" > "VPN". Click "Add VPN profile".

2. Enter "Name" and select "PPTP".

3. Click the VPN profile and enter your username and password to start the connection.

OpenVPN on Windows

1. Download OpenVPN from http://openvpn.net/index.php/open-source/downloads.html/.

2. Install the OpenVPN client on Windows.

The default installation directory is C:\Program Files\OpenVPN.

3. Download the settings files from your QNAP NAS, including the certification file "ca.crt" and the configuration file "openvpn.ovpn".

4. Open "openvpn.ovpn" and replace "OPENVPN_SERVER_IP" with your NAS IP address.

5. Place "ca.crt" and "openvpn.ovpn" in the folder C:\Program Files\OpenVPN\config.

6. Use an administrator account to launch OpenVPN and activate the connection.

Note: If the OpenVPN client is running on Windows 7, add the firewall rules in the advanced settings of OpenVPN.

OpenVPN on Mac OS X 10.11

1. Download and install Tunnelblick from https://tunnelblick.net/.

2. Launch Tunnelblick.

3. Download the settings files from your QNAP NAS, including the certification file "ca.crt" and the configuration file "openvpn.ovpn".

4. Open "openvpn.ovpn" and replace "OPENVPN_SERVER_IP" with your NAS IP address.

5. Double-click the configuration file (or right-click and import the file with Tunnelblick).

The certification file will be imported automatically.

6. Click "Connect".

7. Enter your NAS username and password.

OpenVPN on iOS 9

1. Install OpenVPN Connect from
   https://itunes.apple.com/us/app/openvpn-connect/id590379981?mt=8.

2. Download the settings files from your QNAP NAS, including the certification file "ca.crt" and the configuration file "openvpn.ovpn".

3. Open "openvpn.ovpn" and replace "OPENVPN_SERVER_IP" with your NAS IP address.

4. Open the configuration file with OpenVPN Connect.

Tip: You can send the file to your email address and open it on your device, or you can send the file to the OpenVPN folder via PC with a third-party application such as "iTools for Windows".

5. Enter your NAS username and password

If you have imported the configuration file to the OpenVPN folder you will see it in OpenVPN Connect.

Note: Ensure this option on your iOS device is enabled: "Settings" > "OpenVPN" > "Advanced Settings" > "Force AES-CBC cipher suites".

OpenVPN on Android 5.0

1. Install OpenVPN Connect from
   https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en.

2. Download the settings files from your QNAP NAS, including the certification file "ca.crt" and the configuration file "openvpn.ovpn".

3. Open "openvpn.ovpn" and replace "OPENVPN_SERVER_IP" with your NAS IP address.

4. Import your settings files to the folder on your Android device.

5. Launch OpenVPN Connect and select "Import" in the top-right menu. Find and import the configuration file, and then follow the instructions for importing the certification file.

6. Enter your NAS username and password.

OpenVPN on Windows

1. Download and install OpenVPN from http://openvpn.net/index.php/open-source/downloads.html/.

The default folder for the installation is "C:\Program Files\OpenVPN".

2. Download the settings files from your QNAP NAS, including the certification file "ca.crt" and the configuration file "openvpn.ovpn".

3. Open "openvpn.ovpn" and replace "OPENVPN_SERVER_IP" with your NAS IP address.

4. Place "ca.crt" and "openvpn.ovpn" in the folder C:\Program Files\OpenVPN\config.

5. Use an administrator's account to launch OpenVPN and activate the connection.

L2TP/IPSec on Windows 8

1. Go to "Control Panel" > "Network and Internet" > "Network and Sharing Center" and select "Set up a new connection or network".

2. Select "Connect to a workplace".

3. Select "Use my Internet connection (VPN)".

4. Enter your myQNAPcloud name or IP address in "Internet address".

5. Enter a name for the connection in "Destination name".

6. Go to "Control Panel" > "Network and Sharing Center" > "Change adapter settings".

7. Right-click the VPN connection and select "Properties".

8. Go to "Security", select the "Type of VPN" as L2TP/IPSec, and then click "Advanced settings".

9. Select "Use preshared key for authentication" and enter the same key as the server's settings.

You can now connect to the VPN.

Note: If your NAS is behind a NAT router, use the following configuration:
https://support.microsoft.com/en-us/kb/926179.

L2TP/IPSec on Mac OS X10.10

1. Go to "System Preferences" > "Network".

2. Select "Add new service (+)" and choose "VPN" in "Interface".

3. Select "L2TP/IPSec" in "VPN Type".

4. Enter a name for the connection in "Service Name".

5. Enter your myQNAPcloud name or IP address in "Server Address" and your QNAP NAS user name in "Account Name".

6. Click "Authentication Settings", and enter the password and preshared key.

7. Click "Connect".

L2TP/IPSec on Android 5.0

1. Go to "Settings" > "VPN".

2. Click "Add VPN profile".

3. Enter "Name" and choose the type as "L2TP/IPSec PSK".

4. Enter "IPSec Pre-shared key".

5. Click the VPN profile and enter your username and password.

L2TP/IPSec on iOS 8

1. Go to "Settings" > "General" > "VPN".

2. Choose "Add VPN Configuration…".

3. Select "L2TP".

4. Enter a name for the connection in "Destination".

5. Enter the myQNAPcloud name or IP address in "Server".

6. Enter your QNAP NAS username, password and preshared key.

7. Go to "Settings" > "General" > "VPN" to connect to the VPN.

Privilege Settings

Select the VPN users and specify their privileges.

Add VPN users

Click "Add VPN Users" and check the services you want to allow each user to connect with. Both local users and domain users can be VPN users. You can also search for users in the search bar.

Note: To connect to a VPN server using domain user accounts, you must enable the service in Domain Security.

Delete VPN users

Click "Delete" to remove VPN users. The users will be unable to connect to the VPN service after being deleted.

Connection List

This list shows information about each connection with a server including login time, uptime, username, source IP, VPN client IP, and connection method.

Click "Disconnect" on the table to disable client connections.

VPN Client

The NAS provides the VPN client service which can connect to a VPN server via PPTP, OpenVPN and L2TP/IPSec. The NAS also supports saving multiple VPN settings to easily switch between different connections.

Before you start

Before starting the VPN client service, please ensure that the Internet connection is normal.

Connect a VPN server via PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a commonly-used method for implementing VPN and is supported by most clients, including Windows, Mac OS X, Linux, and mobile devices.

1. Go to "QVPN Service" > "VPN Client".

2. Click "Add" > "PPTP" to connect a VPN server.

3. Enter the connection configuration settings, including the profile name, server address (that you want to connect to), and the username and password of the VPN server.

4. Choose any of the following authentication mechanisms from the "Authentication" menu to protect the VPN client's password during authentication:

o MS-CHAPv2: The password will be encrypted using Microsoft CHAP version 2.

o MS-CHAP: The password will be encrypted using Microsoft CHAP version 1.

o PAP: The password will not be encrypted.

o CHAP: The password will be encrypted using CHAP.

5. If you choose MS-CHAP or MS-CHAPv2, go to the "Encryption" menu and select an option:

o None: The VPN connection will not be encrypted.

o Medium (AES 40/128 bit): The VPN connection will be encrypted using a 40-bit or 128-bit key.

o High (AES 256 bit): The VPN connection will be encrypted using a 256-bit key (the highest-possible level.)

6. Specify the subnet mask.

7. Select any of the following options, as required:

o Use the default gateway on remote network: This will allow all packets to be transferred via the VPN server.

o Allow other network devices to connect to the VPN through the NAS: This will allow network devices on the same LAN as the NAS to connect to the same VPN.

o Reconnect when the VPN connection is lost: This will automatically reconnect to the VPN server when the connection is lost.

8. Select "Create" to start.

> **Note:** To connect to a VPN server using domain user accounts, you must enable the service in Domain Security.

If you select "Allow other network devices to connect to the VPN through the NAS", the network device can access the VPN via the NAS. To enable this function, you must change the default gateway on that other device. Using a Windows PC as an example:

1. Go to "Control Panel" > "Network and Sharing Center" > "Change adapter settings".
2. Right-click the connection icon and choose "Properties".
3. Select "Internet Protocol Version 4 (TCP/IP)" and click "Properties".
4. Choose "Use the following IP address" and change the Default gateway to the IP address of the NAS that is operating the VPN Client service then click "OK".

Connect a VPN server via OpenVPN

The NAS also supports OpenVPN, which is an open-source solution for VPN services. It protects a VPN's connection with the SSL/TLS encrypting mechanism. It is also available on Windows, Mac OS X, Linux, Android and iOS.

To connect to a VPN server via OpenVPN, follow these steps:

1. Go to "QVPN Service" > "VPN Client".
2. Click "Add" > "OpenVPN" to connect to a VPN server.
3. Select the OVPN file (.ovpn) and click "Open".
4. Enter the connection configuration settings, including the profile name, and the username and password of the VPN server.
5. Click inside the required text field to import the certificate (ca.crt) exported from the OpenVPN server.
6. Specify the subnet mask.
7. Select any of the following options, as required:
o Use the default gateway on remote network: This will allow all packets to be transferred via the VPN server.
o Allow other network devices to connect to the VPN through the NAS: This will allow network devices on the same LAN as the NAS to connect to the same VPN.
o Reconnect when the VPN connection is lost: This will automatically reconnect to the VPN server when the connection is lost.
8. Click "Apply" to start.
o If you check "Use the default gateway on remote network", the default gateway on your NAS will change to the VPN server's default gateway.
o If you check "Allow other network devices to connect to the VPN through the NAS", the network device can access the VPN via the NAS.

Connect a VPN server via L2TP/IPSec

1. Go to "QVPN Service" > "VPN Client".
2. Click "Add" > "L2TP/IPSec" to connect a VPN server.
3. Enter the connection configuration settings, including the profile name, server address (that you want to connect to), and the username and password of the VPN server.
4. Choose any of the following authentication mechanisms from the "Authentication" menu to protect VPN client's password during authentication:
   o MS-CHAPv2: The password will be encrypted using Microsoft CHAP version 2.
   o MS-CHAP: The password will be encrypted using Microsoft CHAP version 1.
   o PAP: The password will not be encrypted.
   o CHAP: The password will be encrypted using CHAP.
5. If you choose MS-CHAP or MS-CHAPv2, go to the "Encryption" menu and select an option:
   o None: The VPN connection will not be encrypted.
   o Medium (AES 40/128 bit): The VPN connection will be encrypted using a 40-bit or 128-bit key.
   o High (AES 256 bit): The VPN connection will be encrypted using a 256-bit key (the highest-possible level.)
6. Type the preshared key.
7. Specify the subnet mask.
8. Select any of the following options, as required:
   o Use the default gateway on remote network: This will allow all packets to be transferred via the VPN server.
   o Allow other network devices to connect to the VPN through the NAS: This will allow network devices on the same LAN as the NAS to connect to the same VPN.
   o Reconnect when the VPN connection is lost: This will automatically reconnect to the VPN server when the connection is lost.
9. Select "Create" to start.

Logs

Connection Logs

QVPN Service creates a log entry every time a user accesses a VPN server. The connection logs include the connection method, date, time, username, source IP, and content.

> **Note:** QVPN Service only displays the connection logs. To copy or delete a log, or to export the list, go to "Control Panel" > "System" > "System Logs".

Enable Connection Logs on QVPN Service

1. Open QVPN Service.

2. Go to "Logs" > "Connection Logs".

3. Move the slider to the right.

Event Logs

QVPN Service creates a log entry every time a user enables or disables services, changes settings, and modifies the configuration. The event logs include the date, time, username, and content.

> **Note:** QVPN Service only displays the event logs. To copy or delete a log, or to export the list, go to "Control Panel" > "System" > "System Logs".

Qsync Central

Qsync Central is a cloud-based file synchronization service on the NAS. Simply add files to your local Qsync folder, and they will be available on your NAS and all its connected devices.

In this chapter, the following topics are covered:
- Before you Start
- Starting Qsync Client
- Synchronization
- Sharing
- Remote Access
- Synchronization Management
- Version Control
- Managing or Monitoring Qsync Status via Web Browser
- Using Centralized Mode for Centralized Management

Before you Start

Follow the 5 steps below before Qsync deployment.
1. Create user accounts on the NAS,
2. Downloading Qsync Central on your NAS.
3. Enable home folders for all users.
4. Download the Qsync Client utility on your computers and Qfile on your mobile devices.
5. Log into the NAS (serving as a Qsync server) from your computers or mobile devices (referred to in this document as "Qsync clients".)

1. Creating user accounts on the NAS

- ○ Go to "Control Panel" > "Privilege Settings" > "Users" > click "Create" (or go to "Qsync Central" > "Users" > "Create a User".)
- ○ Only NAS administrators can create accounts.

2. Downloading Qsync Central

1. Go to "Main Menu" > "App Center" to launch App Center.

2. In the search field, type "Qsync".

3. Select "+ Install" under the Qsync Central icon in the search results.

3. Enable Home Folders for All Users

1. Go to "Control Panel" > "Privilege" > "Users" > "Home Folder".

2.   Select "Enable home folder for all users", select disk volume to create folders in. Click "Apply".

4. Downloading Qsync Client

Follow the instructions on the "Overview" page to download the utility for your client device (log into the NAS, click "Qsync Central" on the NAS Desktop > "Overview" page,) or directly download the utility from the QNAP website: "Support" > "Download" > "Utilities".

- ○ For computers, download the Qsync Client utility (only available for Windows.)
- ○ For mobile devices, download and install Qfile from the iOS or Android app stores.

5. Setting up Qsync Client

Launch the installer and follow these steps to set up the Qsync Client:

1. To locate the NAS within a LAN, simply click "Search" or key in its IP address or name (e.g. IP address: 10.8.1.20 or 192.168.1.100.) To connect to a remote NAS (over the Internet) use your myQNAPcloud address (e.g. andy@myQNAPcloud.com.)

2. Enter the NAS login username and password.

3. Set up the Qsync local folder on your PC.

4. Assign a name to identify the local PC for the Qsync server.

5. Click "Apply" .

6. Pair a local folder with the shared folder on the NAS.

Note: If the NAS connection ports have been changed, please append the port number to the IP address; otherwise only enter an IP address. (Default port number: 8080)

Starting Qsync Client

Double click the Qsync shortcut in Windows to open the Qsync local folder. Click the Qsync Client icon on the taskbar to bring up the menu. If you copy/move files to the local Qsync folder on one of your devices, the files will be synced with all the other devices (devices with the Qsync Client installed that are connected to the NAS.) From now on, there is no need to copy files back-and-forth between your PC and these other devices or worry about the size of files as you try to attach them to an email.

Synchronization

There are several methods for synchronizing files. Qsync Central will automatically synchronize the files across your computers and mobile devices that have the Qsync Client installed, and they will also be synchronized to the Qsync folder on the NAS:
 1. For PCs, drag and drop files to the local Qsync folder.
 2. For mobile devices (Qfile), copy or move files into the local Qsync folder.
 3. For the NAS, copy or move files to the Qsync folder using File Station.

> **Note:**
> - If files are "dragged and dropped" to the local Qsync folder, they will be moved (and not copied) to that folder if the files and the local Qsync folder are on the same disk drive. This behavior is the same as Windows File Explorer.
> - The maximum size of a single file that Qsync can transmit across a LAN is 50GB.
> - Qsync does not support SAMBA, FTP or AFP for files access. Please access files using File Station or a Qsync Client.
> - Qfile only synchronizes the file list and does not download the files to a mobile device. Please download the files when you need them.

Offline editing
You can edit your files offline and Qsync Central will automatically synchronize the changes made once your device is online.

Sharing

Sharing files by download links
You can share files by sending download links to those who have not installed Qsync Client.

For Windows:
 1. Right click on the file that you want to share in the local Qsync folder and click "Share the link".

2. Choose to send the link via email or copy the link to directly share it.
3. Click "Settings" to see more options, including creating a SSL link, the expiration date, or password.

For the NAS, right click on the file that you want to share in the Qsync folder within File Station and click "Share".

For mobile devices, launch Qfile to share the file in the local Qsync folder by clicking the icon to the right and click "Share".

The file recipients can click the link or copy and paste it to a web browser to download the file.

Sharing folders with a group

You can share a folder with a user group. If any member from the group shares the files in the folder, other members can receive the file.

1. Create user accounts in the NAS for each group member.
2. Ensure that a Qsync Client is installed on each member's device.
3. Right click on the folder you want to share in the local Qsync folder and click "Share this folder as a team folder".
4. Select users from the list of local or domain users.

All of the members in the group will receive a file sharing invitation. Once accepted, the group members can start accessing this shared folder.

> **Note:**
> - The team folder will only take effect after users accept their invitation.
> - Users cannot share team folders that have been shared with them.
> - Only the folders under /home on your NAS can be shared as a Team Folder.

Remote Access

Accessing the NAS over the Internet

To connect to a remote NAS (over the Internet), the administrator must first configure the device name for the NAS in "myQNAPcloud". The administrator can then share the myQNAPcloud address to allow users to access the remote NAS. (e.g. andy@myQNAPcloud.com)

> **Note:**

- A connection with a NAS over the Internet will be slower compared to a LAN environment.
- As you switch back to a LAN-based NAS, ensure that you reconnect to the NAS via LAN to get a better connection quality.
- To improve file transmission performance, it is recommended that you configure port forwarding on the router.

Synchronizing photos and videos automatically

Qsync Central can synchronize your photos and videos from mobile devices to the Qsync folder across all Qsync client devices.
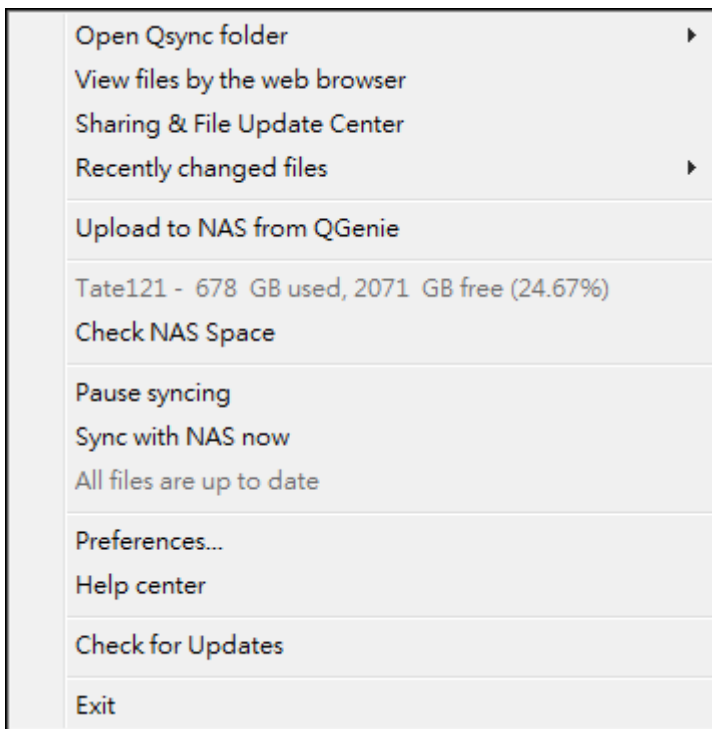
Steps:
1. Install Qfile on your mobile devices by following instructions outlined on the Qsync Central Overview page on the NAS or find it from your device's app store.
2. Launch Qfile.
3. Click "Settings" on the bottom-right side of the screen.
4. Scroll down and look for "Auto upload from photo gallery" and click on "Set up now".
5. Select a NAS to upload photos and videos to.
6. Select the folder.
7. Select "Use default setting" (/Qsync/Camera Uploads) or select "Set up manually" to set the path.
8. Select if you want to upload all photos from the photo gallery immediately.
9. You can tick the checkbox "Limit to Wi-Fi" to ensure that you only upload files through Wi-Fi and not your phone's network.
10.   The uploaded files will be synchronized to the "Camera Uploads" folder under the Qsync folder on Qsync client devices.

Note: If files that were previously uploaded are deleted from the "Camera Uploads" folder, Qfile will not upload those copies in the photo library again.

Synchronization Management

Click the Qsync Client icon on the taskbar to see the management functions:

```
Open Qsync folder                               ▶
View files by the web browser
Sharing & File Update Center
Recently changed files                          ▶

Upload to NAS from QGenie

Tate121 - 678 GB used, 2071 GB free (24.67%)
Check NAS Space

Pause syncing
Sync with NAS now
All files are up to date

Preferences...
Help center

Check for Updates

Exit
```

1. Add files and view the synchronization result on the NAS:

   a. Open Qsync folder: Open the local Qsync folder to add files.

   b. View files by the web browser: Browse files in the Qsync folder using File Station.

2. Control synchronization progress:

   a. Pause syncing / Resume syncing: Click to pause or resume syncing.

   b. Sync with NAS now: Force Qsync to scan again and refresh the synchronization list.

3. Information for syncing and sharing:

   a. Sharing & File Update Center

      i. File Update Center: List the file or folder update logs.

      ii. Sharing Center: List the folders or files shared with others. Users can choose to accept or decline the team folders. However, users cannot share team folders that are shared by others.

   b. Recently changed files: Lists the recently updated files.

4. Preference:

   a. General:

      i. Link Status: Shows the current status. Click "Logout" to change users.

      ii. Network Recycle Bin: Browse or recover files deleted from the Qsync folder.

   b. Sync:

      i. Manage paired folders: Add, delete, or edit folder pair settings.

      ii. Import photos and videos: Import photos and videos when an USB device is connected. This feature only checks for photos and videos in the "DCIM" folder in the root directory of USB devices.

      iii. Default folder: choose a folder to import files from external drives or QGenie.

iv. Do not remove any files on the NAS when synchronizing: You can remove files within the local Qsync folder, and files deleted from your computer will not be synchronized with the NAS. The NAS will still retain copies of deleted files.

c. Policy:

   i. Conflict Policies: The policies for handling the name conflicts between the Qsync server (NAS) and clients after it is back online from a disconnection:

      1) Rename the local files,

      2) Rename the remote NAS files,

      3) Replace local files with remote NAS files, or

      4) Replace remote NAS files with local files.

   ii. Sharing Policies: The policies of the team folders when other Qsync users share them to this local computer:

      1) Always reject sharing,

      2) Automatically accept sharing, or

      3) Send a notification message once sharing occurs.

   iii. Filter Settings: During file synchronization, Qsync will skip the file types specified in filter settings.

d. E-Mail:

   i. Set up E-mail: Set up an email account for sharing file links. You can use the NAS SMTP server settings (for administrators only), your PC's mail server settings, or configure a new SMTP server.

e. Proxy:

   i. Set up Proxy: Use a proxy server for the Qsync client device.

f. Advanced:

   i. Debug log: The system will record all of the synchronization activities between your computer and the NAS for diagnosing technical problems.

Note: The "Sync" and "Proxy" tab is not available on Mac.

Version Control

This will retain one copy of a file as a version whenever you add or modify it, allowing you to retrieve a specific previous version at any time. Or, if you accidently overwritten a previous version made by others while editing the file in team folder, you can still restore the previous version. And you can restore the previous versions even if you have deleted the file from the recycle bin.

Viewing the version history
You can view the version history by using File Station. Right click on a file or folder in the Qsync folder in File Station and select "Previous Versions" to show the version list (or you

can access it from menu bar "More Action" > "Previous Versions". Or, just click the "Show Right Panel" > "Version". You can also access it from the Qsync client utility. Right click on a file of folder in the Qsync folder and select "Previous Versions".

Restoring the previous versions

In the version history page, select the version you want to restore and click "Restore".

- Click "Download" to download the version to the local computer.
- Click "Delete All" to delete all of the listed versions.
- Click "Refresh" to update the status of the version history.

Restoring versions of a deleted file

Version control retains versions in a separate location, so even you delete the file, you can still restore the previous versions of the file - even if the file has been deleted from the recycle bin.

To restore the version of a deleted file, click on any folder/file in the Qsync folder, and then click "More Action" > "Show Deleted Files" in the menu bar. To view the version history, right click on a file/folder in Qsync folder and select "Previous Versions". Or you can access it from the menu bar, "More Action" > "Previous Versions". Or just click the "Show Right Panel" > "version" to show the version list.

Restoring previous versions

In the version history page, select the version you want to restore and click "Restore".

- Click "Download" to download the version to the local computer.
- Click "Delete All" to delete all of the listed versions.
- Click "Refresh" to update the status of the version history.

> **Note:** If you click "Delete All", then click "Refresh" and the associated files will be removed from the list.

To exit the view of the deleted file list, right click on any file/folder and select "Hide Deleted Files". Or access it from menu bar, "More Action" > "Hide Deleted Files".

Managing and setting version control

To access the management and settings of version control, click the Qsync button on the desktop of the NAS, then click "Version Control" in the right-side menu.

The target folder

"Enable version control" is the main switch of the version control. Disabling this option will not delete versions that have already been created. "Enable version for my Qsync folder" allows each user to apply the function to their files.

Target folder for version control

You can apply the version control to the files under specific Qsync folders to save space. To assign specific folders, select "Assign specific subfolder under the Qsync folder", then click "Add" to add folders. You can add up to 5 folders. Click "Delete" to remove all versions under the selected folders and subfolders. This will not take effect until you click "Apply" or "Apply All".

Advanced

Maximum Number of Versions: You can choose how many versions you want to retain. This is a control only for administrators. The more versions you keep the more storage space will be taken up. To know how much space has been used for version control, click "Check" in the "Disk Used for Version Control" section.

Note:

- If you reduce the maximum number of versions, it will impact the versions that have been created and if the volume of versions exceeds the new settings, the earlier versions will be dropped. Only the equivalent number of latest versions as of the new settings will be kept.
- The deletion will only take effect after you click "Apply" or "Apply All".
- The maximum number of versions supported for Version Control is 64.

Managing or Monitoring Qsync Status via Web Browser

Log into the NAS via web browser and click Qsync Central.

1. Overview: This page shows the mode of use management (User Customization Mode or Central Configuration Mode) and the total number of online users and devices. It also provides links to File Station and for installing Qsync. In addition, you can enable or disable the Qsync service (for administrators only.)
2. Management settings: This provides a centralized management for administrators to edit Qsync Client default settings. For details on the management settings, please refer to the Using Centralized Mode for Centralized Management section.
3. Users: Lists the information of online users, and you can manage the users of Qsync service here (for administrators only.)
4. Devices: This table lists the status of connected devices. It also provides options for you to manage each device, allowing you to edit their settings, block them, or to remotely erase them.
   a. If users log in from their PC, the name of the device will be shown as their computer name.

    b. If users log in from Qfile, the name of the device will be shown as "Qfile-Android" or "Qfile-iPhone".

    c. If users move or copy files to the Qsync folder in the File Station, the name of the device will be shown as "Qsync-File Station".

5. Event Logs: Lists activity details by user.

6. Team Folder: Lists information about team folders, including folders that you shared and folders that are shared with you.

7. Shared Folder: Administrators can decide which shared folders will be synced with client devices. If a user has Read/Write or Read-only and synchronization privileges on a shared folder, it can then be synced with their client device.

8. Shared File Links: Lists the status of shared links.

9. Version Control: You can set the maximum number of version for your files and check the space used for Version Control.

Using Centralized Mode for Centralized Management

Administrators can now apply pre-configured settings to devices that connect to the NAS for the first time, restrict users' right on modifications to all or certain preference settings of their client utilities, edit settings for individual Qsync client devices online, or set a management password (a master password for all client devices.)

To apply pre-configured settings on connected devices, follow these steps:
1. Log into the NAS as an administrator > "Qsync Central" > Management settings,
2. Click "Edit default settings".
3. Under the "Synchronize" tab, choose whether to remotely remove any files on the NAS during synchronization.
4. Under the "Policy" tab, set conflict policies, and filter settings.
5. Under the "Mails" tab, set up the email option and sender details.
6. Click "Apply".

To allow all users to configure their own client utility, follow these steps:
1. Log into the NAS as an administrator > "Qsync Central" > Management settings,
2. Select "Central Configuration Mode" and tick the preference settings that users are allowed to modify for their Qsync client device.
3. Click "Apply".

To edit settings for individual Qsync client devices, follow these steps:
1. Log into the NAS as an administrator and navigate to the "Devices" page in Qsync Central.
2. Click the "Edit settings for Qsync utility" icon under "Action" for the device to be modified
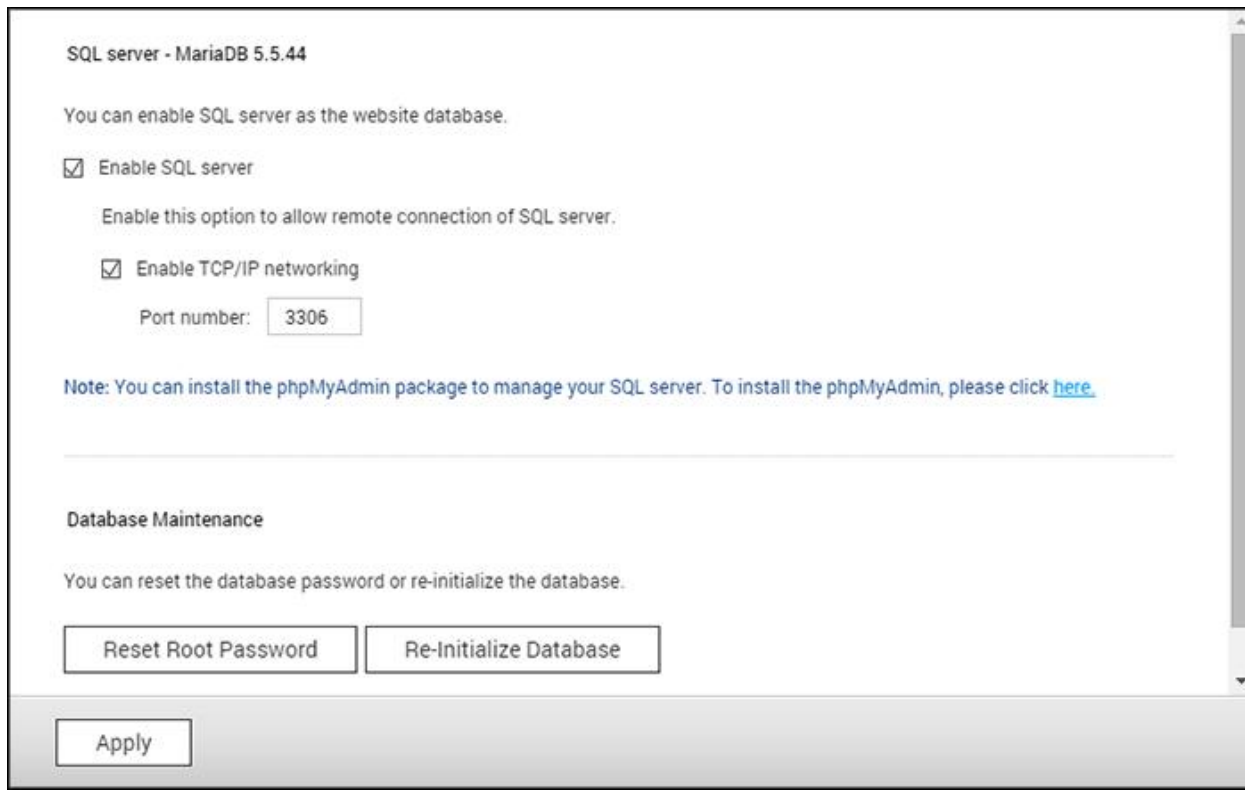
3. Modify its preference settings (including synchronization, policy and mail settings.)

To set a management password, follow these steps:

1. Log into the NAS as an administrator and navigate to the "Management Settings" page in Qsync Central.
2. Select Central Configuration Mode.
3. Tick "Enable your management password".
4. Enter the password and click "Lock".

SQL Server

You can enable an SQL Server to be a website database.

Note: For legacy ARM models (TS-x21, TS-x20, TS-x19, TS-x12 and TS-x10), MySQL will still be used as the default SQL server. If you are using a legacy ARM model, you can still install MariaDB from the App Center.

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. If this option is disabled, your MySQL server will only be configured as a local database server for the web server of the NAS. After enabling remote connection, assign a port for the remote connection service of the MySQL server. The default port is 3306. After the first-time installation of the NAS, a phpMyAdmin folder 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.
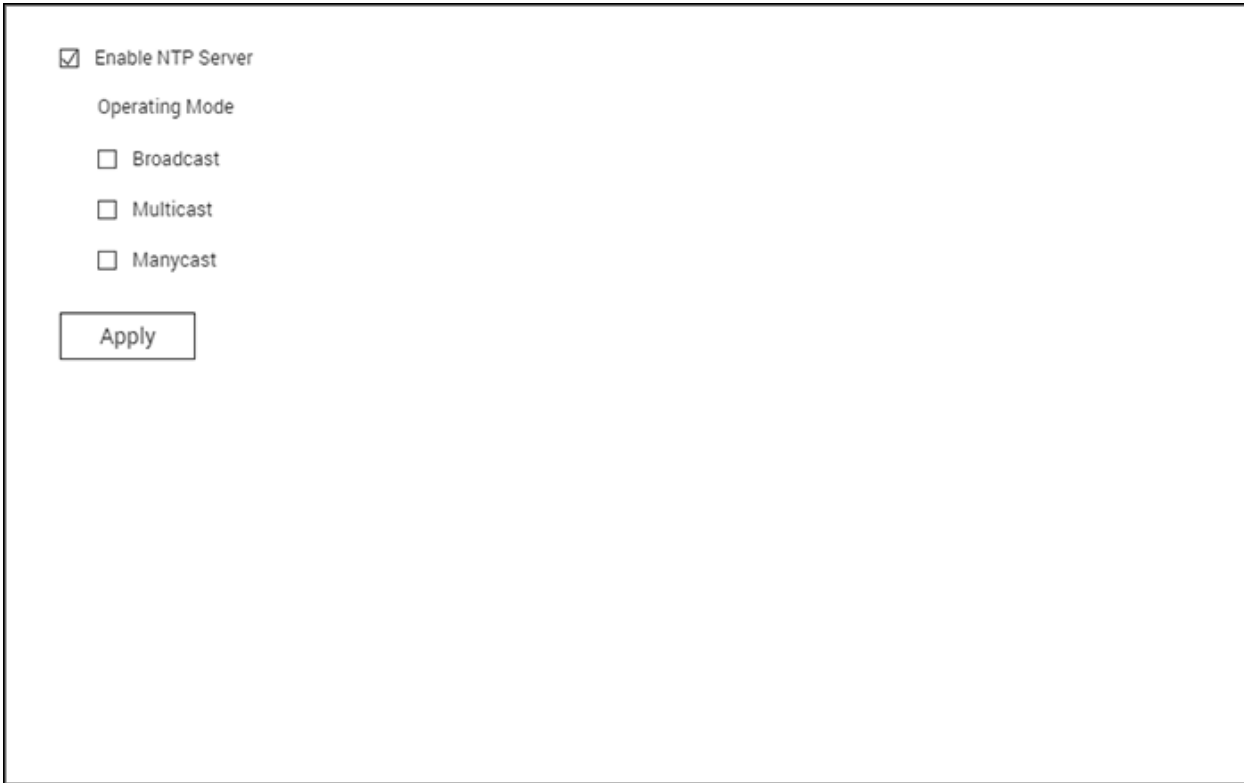
Database Maintenance

o   Reset root password: Reset the password of MySQL root as "admin".

o   Re-initialize database: Delete all the data on the MySQL database.

Note:

- To use this feature on the TS-x39/509/809 series NAS, 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.
- Do not delete the phpMyAdmin folder. You can rename the 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 will remain unchanged.

NTP Service

A NTP Server allows the PCs, servers and other network devices to synchronize their time with the same reference: the NAS. It is useful (and sometimes required) to keep the time synchronized for all devices in some environments.

Setting up NTP Server

To set up the NTP Server, first go to "Control Panel" > "Applications" > "NTP Service" and check "Enable NTP Server". Select to check the following three operating modes:

- Broadcast: This will allow the NTP server to periodically send broadcast packets with the IP address "255.255.255.255 ". Clients compatible with this mode can use this to synchronize their time.
- Multicast: This will allow the NTP server to periodically send multicast packets. Clients compatible with this mode can use this to synchronize their time. Specify the multicast IP address after this option is enabled.
- Manycast: This will allow the NTP server to listen for manycast requests from NTP clients and reply to the client requests received. Specify the manycast address after this option is enabled.

> **Note:** For multicast and manycast modes, the NTP clients will only receive this kind of packets after they are configured for the modes. Please refer to their user manuals for setup details.

RADIUS Server

The NAS can be configured as a RADIUS (Remote Authentication Dial In User Service) server to provide centralized authentication, authorization, accounting management for computers to connect and use a network service.

To use this feature, follow these steps:

1. Enable RADIUS Server on the NAS in "Control Panel" > "Applications" > "RADIUS Server" > "Server Settings". Click "Apply".
2. Add RADIUS clients, such as Wi-Fi access points and VPN, on the NAS in "RADIUS Server" > "RADIUS Clients". Up to 10 RADIUS clients are supported. Click "Create a Client".
3. Enter the client information and click "Apply".
4. The clients are shown on the list.
5. Create RADIUS users and their password in "Control Panel" > "Applications" > "RADIUS Server" > "RADIUS Users". The users will be authenticated when trying to access the network through RADIUS clients. The maximum number of RADIUS users the NAS supports is the same as the maximum number of local NAS users supported. See the chapter on Users for details. Click "Create a User".
6. Enter the username and password. The username only supports letters (a-z and A-Z) and numbers (0-9). The password must be 8-32 characters in length.

7. Specify to grant dial-in access to local NAS users. Enable this option to allow local NAS users to access network services via RADIUS clients using their NAS login name and password.

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

Syslog Server

Configure the NAS as a Syslog server, create Syslog filters and view available Syslog messages on this page.

Server Settings

- **Server Settings:** To configure the NAS as a Syslog server and allow it to receive Syslog messages from clients, enable Syslog Server. Select the protocols (TCP and/or UDP) the NAS uses to receive Syslog messages. Specify the port numbers if necessary or use the default port number 514. Click "Apply" to save the settings. After enabling the NAS as a Syslog server, enter the NAS IP as the Syslog server IP on the Syslog clients to receive Syslog messages from them.
- **Log Settings:** Specify the maximum log size (1-100 MB) of Syslog messages, the location (NAS shared folder) where the logs will be saved, and the file name. Once the logs have reached their maximum size, the log file will be automatically archived and renamed with the archive date as MyLogFile_yyyy_mm_dd, for example MyLogFile_2011_12_31. If multiple log files are archived on the same day, the file will be named as MyLogFile_yyyy_mm_dd.[number]. For example, MyLogFile_2011_12_31.1, MyLogFile_2011_12_31.2, and so on. Click "Apply" to save the settings.
- **Email Notification:** The NAS supports sending email alerts to up to 2 dedicated email addresses (configured in "System Settings" > "Notification" > "Alert Notification") when

the severity of the received Syslog messages match the specified level. To use this feature, configure the SMTP server settings in "System Settings" > "Notification" > "SMTP Server". Next, enable email notification and select the severity level in "Applications" > "Syslog Server" > "Server Settings". Click "Apply" to save the settings.

Severity	Level (smallest number the highest)	Description
Emerg	0	Emergency: the system is unusable. Alert emails will be sent when Syslog messages of levels 0-4 are received.
Alert	1	Alert: immediate action required. Alert emails will be sent when Syslog messages of levels 1-4 are received.
Crit	2	Critical: critical conditions. Alert emails will be sent when Syslog messages of levels 2-4 are received.
Err	3	Error: error conditions. Alert emails will be sent when Syslog messages of levels 3-4 are received.
Warning	4	Warning: warning conditions. Alert emails will be sent when Syslog messages of level 4 are received.

Filter Settings

This feature should only be operated by administrators who are familiar with Syslog filters. Follow these steps to create Syslog filters for the NAS to receive Syslog messages that match the criteria:

1. Click "Add a Filter".
2. Define the filter settings and click "Add". To edit the filters or to manually add filters, click "Manual Edit" and modify the contents in the dialog. Click "Apply" to save the filter.
3. The filters will be shown on the list. The NAS will only receive Syslog messages that match the filters which are in use.
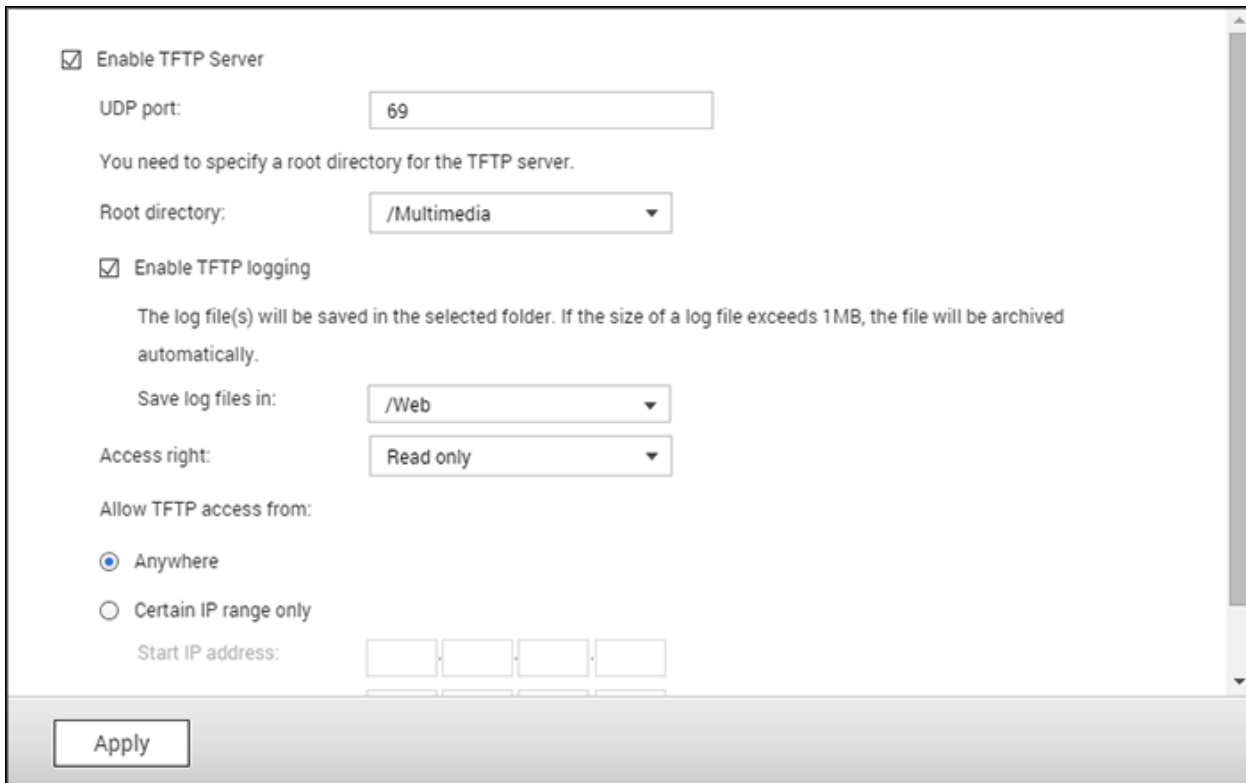
Button	Name	Description
▶	Enable	Enable a filter
⏸	Disable	Disable a filter
📝	Edit	Edit filter settings
Delete	Delete	Delete filters

Syslog Viewer

Use the Syslog viewer to view the available Syslog messages on the NAS. Select to view the latest logs or the logs in a particular archived file. Log files can be accessed on the directory configured in "Syslog Server" > "Server Settings" > "Log Settings".

TFTP Server

Configure the NAS as a TFTP (Trivial File Transfer Protocol) server for configuration management of network devices and remote network booting of computers for system imaging or recovery. TFTP is a file transfer protocol with the functionality of a very basic form of FTP. TFTP does not provide user authentication and cannot be connected to using a standard FTP client.

Follow these steps to use this feature:
1. Select "Enable TFTP Server".
2. The default UDP port for file transfer is 69 and you should only change it if necessary.
3. Specify a folder on the NAS as the root directory of the TFTP server.
4. Enable TFTP Logging: Enable this option and specify the directory to save the TFTP log file (opentftpd.log.) It is recommended to view the log file using Microsoft Excel or WordPad on Windows OS or by TextEdit on Mac OS.
5. Assign read only or full access to the clients.
6. Restrict the TFTP client access by specifying the IP address range or select "Anywhere" to allow any TFTP client access.
7. Click "Apply".

Note: To set up PXE with your NAS, please use a static IP for your NAS, enable its DHCP service and specify the TFTP server IP and name of the boot file in "Control Panel" > "Network" > click the "Edit" button next to the LAN port > "DHCP server". For more details, please refer to the DHCP Server chapter

Virtualization

QNAP business-class Turbo NAS is a virtualization-ready storage solution designed to optimize your virtualization operations. In addition to the support for VMware vSphere, Microsoft Hyper-V and Citrix XenServer, this storage solution includes the cutting edge VAAI for iSCSI, VAAI for NAS and ODX (Offloaded Data Transfer) technologies to offload the heavy-duty file operations from the servers and flexible volume management approaches, such as Thin Provisioning and Space Reclaim, to manage your volumes more effectively. To double system performance, QNAP offers a number of network accessories that support 10GbE and 40 GbE transmission speeds, Qtier™ technology and SSD Cache feature that capitalize on SSD technologies for auto-tiering and SSD caching. Besides, the QNAP vSphere Client plugin, QNAP vSphere Web Client plugin, QNAP Snapshot Agent and QNAP SMI-S Provider are available to increase management productivity and efficiency.

Note: Each feature mentioned in this chapter is applicable only to specific models. Please refer to each respective section for supported models.

Server Virtualization

The Turbo NAS supports three types of server virtualization applications: VMware vSphere, Microsoft Hyper-V and Citrix XenServer. For details on each of the solutions and supported models, check here.

VAAI for iSCSI and VAAI for NAS

The Turbo NAS supports VMware VAAI (vStorage APIs for Array Integration) to increase operational performance in virtualization environments. With VAAI, data processing is offloaded to the Turbo NAS, and standard virtual machine management and deployment can be performed more efficiently, consuming less ESXi CPU, memory, and bandwidth resources. VAAI includes two parts: 1) VAAI for iSCSI and 2) VAAI for NAS.

VAAI for iSCSI supports the following four features:
- **Full Copy (hardware-assisted copy):** Processes the full copies of data within the Turbo NAS without requiring that the EXSi host reads and writes the data. This feature can reduce the loading for ESXi hosts and speed up the cloning process for virtual machines;
- **Block Zeroing (hardware-assisted zeroing):** Enables Turbo NAS to zero out a large number of blocks to speed up the provisioning of virtual machines. This feature can reduce the loading for ESXi hosts and increase capacity allocation efficiency for virtual machines;

- **Hardware-assisted Locking:** Enables granular locking of block storage devices rather than locking the entire LUN in SCSI. This feature permits the VMware vSphere environment to scale up for more virtual machines and more ESXi hosts without performance penalty and boosts efficiency when a single datastore is shared by a number of ESXi hosts;
- **Thin Provisioning with Space Reclaim:** Releases the LUN space when virtual disks are deleted or migrated. This feature can report disk space consumption more accurately, avoid out-of-space conditions, increases NAS space utilization and saves IT cost.

VAAI for NAS offers the following three features:
- **Full File Clone:** Enables the Turbo NAS to copy all data within the NAS without requiring that the ESXi host reads and writes the data. This feature can reduce loading for ESXi hosts, speeds up the cloning process for virtual machines.
- **Extended Statistics:** Enables vSphere to query space utilization details for virtual disks on QNAP NFS datastores, including the size of a virtual disk and the real space consumption of that virtual disk. This feature can report disk space consumption more accurately, increase NAS space utilization and save IT cost.
- **Reserve Space:** Reserves the pre-allocated space of virtual disks (thick provision eager zeroed disks) in QNAP NFS datastores. This feature can increase virtual disk read/write performance (thin provision disks vs. thick provision disks.)

With the support of VAAI for iSCSI and VAAI for NAS, the Turbo NAS can boost storage performance (more than 120 times faster) to create new virtual machines in a virtualized environment. For more details on VAAI for iSCSI and VAAI for NAS, check here.

ODX (Offloaded Data Transfer)

The Turbo NAS supports Offloaded Data Transfer (ODX) in Microsoft Windows Server 2012, making it a high performance iSCSI storage solution in Hyper-V virtualized environment. Supporting ODX, the Turbo NAS can be offloaded with all the copying processes from Windows servers. It highly reduces loading of Windows servers and improves the performance of copying and moving operations for Windows 2012 hosts using the QNAP iSCSI storage. For more details on ODX, check here.

10 GbE and 40 GbE Support

A 10GbE (10 Gigabit Ethernet) and 40 GbE network is essential for businesses that demand high bandwidth for virtualization and fast backup and restoration efficiency for an ever-growing amount of data. QNAP's 10GbE Turbo NAS series is an affordable and reliable storage solution for deploying a 10GbE environment. For detail on 10GbE and 40 GbE support, its application, technical specifications (physical interfaces), applications and the compatibility list, check here.

SSD Cache

Based on the SSD technology, the SSD cache feature is designed to boost access performance of the Turbo NAS. As the name "SSD Cache" implies, SSD drives need to be installed to enable this function. To learn how to set up SSD Cache on the Turbo NAS, check here.

Qtier™ Technology

Based on the SSD technology, Qtier is designed to boost access performance of the Turbo NAS. Qtier can optimize your data based on the access pattern and then automatically move the data to a suitable hard drive. Qtier supports two to three tiers, which can be SSD drives, SAS drives or SATA drives. SSD drives are required to enable this function. To learn more about Qtier on the Turbo NAS, check here.

QNAP vSphere Client Plugin and vSphere Web Plugin

The QNAP vSphere Client plugin for QNAP Turbo NAS is an interface between ESXi and the Turbo NAS. This tool allows system administrators to manage VMware datastores on the QNAP Turbo NAS directly from the vSphere Client console and verify the status of all QNAP Turbo NAS units. For setup details on vSphere Client,, check here.

QNAP SMI-S Provider

QNAP SMI-S Provider is a required component for the support of System Center Virtual Machine Manager (SCVMM 2012 and 2012 R2). With this tool, the Turbo NAS can directly communicate with SCVMM 2012, and server management tasks can be facilitated for administrators. For detail on QNAP SMI-S Provider, check here.

Web Server

Go to "Control Panel" > "Applications" > "Web Server" to configure the web server and virtual host.

Web Server

The NAS can host web sites including those that use Joomla!, PHP and MySQL/SQLite to establish an interactive website. To use the Web Server, follow these steps.

1. Enable the service and enter the port number. The default number is 80.
2. Configure other settings:
   a. Maintenance: Click "Restore" to restore the web server configuration to default.
   b. php.ini Maintenance: Choose to upload, edit or restore php.ini.
3. Secure Connection (HTTPS): Enter the port number for SSL connection.
4. Upload HTML files to the shared folder (Qweb/Web) on the NAS. The file index.html, index.htm or index.php will be the home path of your web page.
5. You can access the web page you upload by entering http://NAS IP/ in the web browser. When the Web Server is enabled, you must enter http://NAS IP:8080 in your web browser to access the NAS login page.

> **Note:**
> - If the Web Server is disabled, all relevant applications including Music Station, Photo Station, Happy Get, or QAirplay will become unavailable.
> - To use PHP mail(), go to "System Settings" > "Notification" > "SMTP Server" and configure the SMTP server settings.

WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to the HTTP(S) protocol that allows users to edit and manage files collaboratively on remote servers. After enabling this function, you can map shared folders of your NAS as network drives of a remote PC over the Internet. To edit the access rights, go to "Privilege Settings" > "Shared Folders" page.

> **Note:** WebDAV currently supports NAS user accounts and AD domain user accounts. LDAP user accounts are not supported.

To map a NAS shared folder as a network drive on your PC, enable WebDAV and follow these steps.
1. Go to "Privilege Settings" > "Shared Folders". Click "Access Permissions" for the designated folder under the "Action" column.
2. Select "WebDAV access" from the dropdown menu on the top of the page and specify the access rights. Choose the authentication level or scroll down to search for the account to grant its access rights. Click "Apply".
3. Next, mount the NAS shared folders as the shared folders on your computer using WebDAV.

Windows Vista
If you are using Windows Vista, you may need to install "Software Update for Web Folders (KB907306)". This update is only for 32-bit versions of Windows Vista.
http://www.microsoft.com/downloads/details.aspx?FamilyId=17c36612-632e-4c04-9382-98 7622ed1d64&displaylang=en

1. Right click on "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 NAS URL with the folder name. Format:
   http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME
5. Enter the account login details that have WebDAV access rights to connect to the folder.

6. Enter a name for this network place.

7. The Web folder has been successfully created.

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

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

Mac OS X

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

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

1. Open "Finder" > "Connect to Server", and enter the URL of the folder. Format:

   http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME

2. Enter the account login details that have WebDAV access rights to connect to the folder.

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

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

These instructions are based on Mac OS X 10.6, and can be applied to 10.4 or later.

Ubuntu

Follow these steps 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 account login details that have WebDAV access rights to connect to the folder. Click "Connect" to initialize the connection.

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

MySQL Management

Install phpMyAdmin and save program files in the Web or Qweb share of the NAS. You can change the folder name and connect to databases by entering the URL in the browser.

> **Note:** The default username of MySQL is "root". The password is "admin". Change the root password **immediately** after logging in to the phpMyAdmin management interface.

SQLite Management

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

1. Unpack the downloaded file SQLiteManager-*.tar.gz.

2. Upload the unpacked folder SQLiteManager-* to \\NAS IP\Web\ or \\NASIP\Qweb.

3. Open a web browser and go to http://NAS IP/SQLiteManager-*/.?:

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

Virtual Host

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

Before you Start

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

Host name	WAN/LAN IP and port	Document root	Demo web application
site1.mysite.com	WAN IP: 111.222.333.444 LAN IP: 10.8.12.45 (NAS) Port: 80 (NAS)	/Qweb/site1_mysite	Joomla!
site2.mysite.com		/Qweb/site2_mysite	WordPress
www.mysite2.com		/Qweb/www_mysite 2	phpBB3

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

- Web Server: Enable Web Server in "Applications" > "Web Server".
- DNS records: The host name must point to the NAS WAN IP. You can normally configure this from your DNS service providers.
- Port forwarding: If the web server listens on port 80 you need to configure port forwarding on your router to allow inbound traffic from port 80 to the LAN IP (10.8.12.45) of your NAS.
- SSL certificate import: If you are going to enable SSL connection for the website and intend to use your own trusted SSL certificates you can import certificates from within the administration backend under "System Settings" > "Security" > "Certificate & Private Key".

Using Virtual Host

Follow these steps to use virtual host:
1. Select "Enable Virtual Host" and click "Apply".
2. Click "Create a Virtual Host".
3. Enter the host name and specify the folder where the web files will be uploaded to.

4. Specify the protocol (HTTP or HTTPS) for connection. If you select HTTPS, make sure the option "Enable Secure Connection (SSL)" in Web Server has been enabled.
5. Specify the port number for connection.
6. Click "Apply".
7. Continue to enter the information for the rest of the sites you want to host on the NAS.
8. Create a folder for each website (site1_mysite, site2_mysite, and www_mysite2) and start transferring the website files to the corresponding folders.
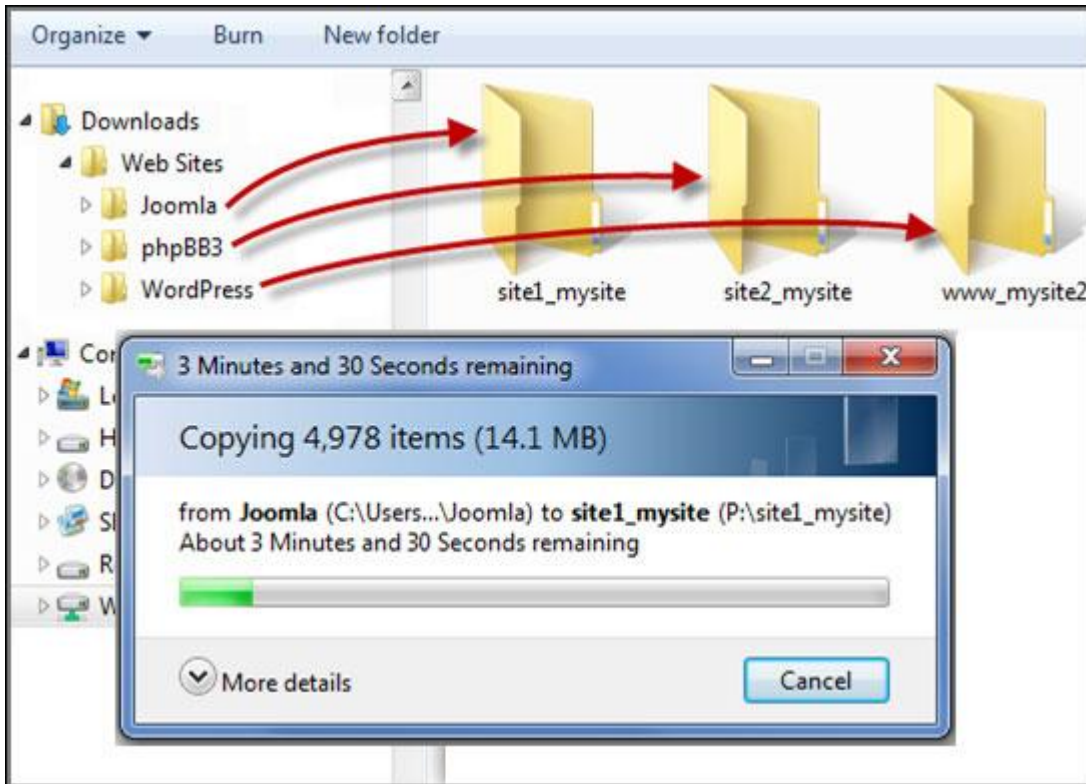
Once the files transfer is complete, point your web browser to the websites by http://NAS_host_name or https://NAS_host_name according to your settings. In this example, the URLs are:

- http://site1.mysite.com
- http://site2.mysite.com
- http://www.mysite2.com

Using the above example, you would see the Joomla!, phpBB3, and WordPress sites respectively.

Other Applications

Various applications are provided by QNAP to enhance your user experiences. For details on these applications, refer to the following links:

- [App Center](#)
- [DLNA Media Server](#)
- [Download Station](#)
- [Helpdesk](#)
- [HybridDesk Station](#)
- [iTunes Server](#)
- [Multimedia Management](#)
- [Music Station](#)
- [myQNAPcloud Service](#)
- [Photo Station](#)
- [Video Station](#)

App Center

The App Center is a platform for the distribution of NAS apps. Users can search for, install, remove and update apps developed by QNAP and third-party developers to expand services and add new features to the NAS.
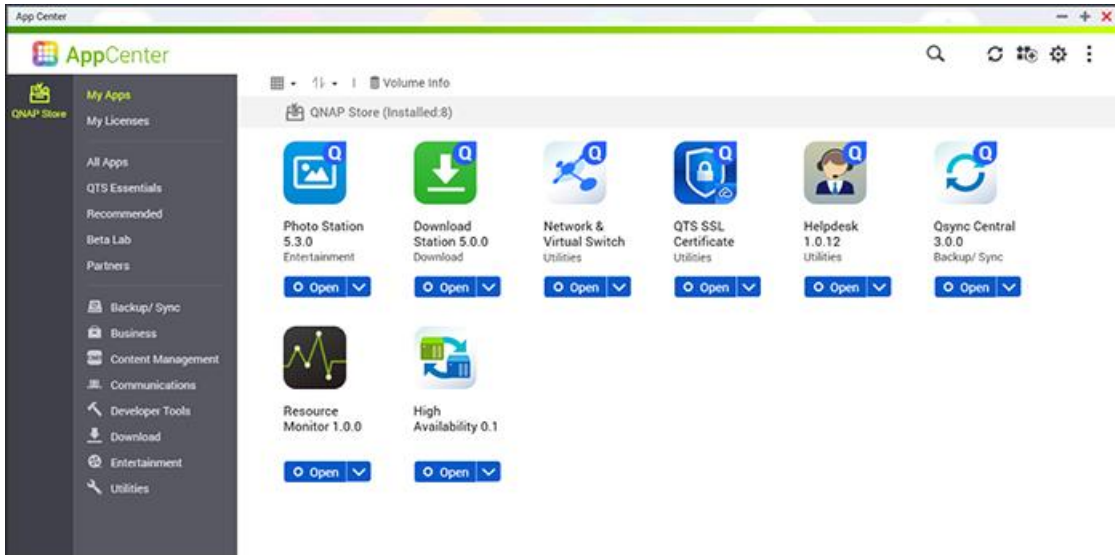
Starting App Center

The App Center can be launched from the App Center shortcut on the Main Menu or the NAS Desktop.

Familiarizing yourself with App Center

Menu Bar
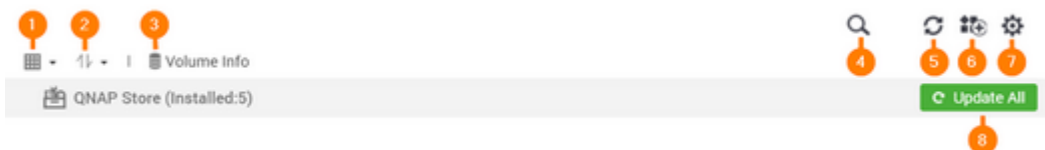
No	Name	Description
1	View Mode	Switch to item mode or list mode for the apps.
2	Sort	Sort apps by category, name, or release date, in an ascending or descending fashion.
3	Volume	Check the following volume information for currently installed apps: free

	Info	and total storage capacity, associated storage pools, RAID Group, disks, and apps already installed on each volume.
4	Search	Search for apps that are available to install on the NAS.
5	Refresh	Check for the latest updates.
6	Manual Install	Browse to upload and manually install a QPKG add-on. You can also find information on App add-on developments [here]().
7	Settings	• App Repository: If you have an URL provided by a third-party community or developer, you can add or modify it here to import applications from other sources. • Update: QTS can automatically update or send notifications when there are app updates available. You can choose between being notified via email, push notification on your QTS desktop, or both.
8	Update All	Update all of the Apps that are currently installed on the NAS

Left Panel

- My Apps: List Apps that are currently installed on the NAS.
- My Licenses: List licenses for all Apps to be installed on the NAS. You can also add and activate your licenses.
- All Apps: List all Apps that can be installed on the NAS.
- QNAP Essentials: List Apps developed by QNAP.
- Recommended: List Apps recommended by QNAP (they could be either developed by QNAP or third party developers.)
- Beta Lab: Lists Apps that are currently in development.
- Partners: List Apps developed by QNAP partners.
- Apps by types: From "Backup/Sync" to "Education", those are App categories listed to facilitate your App searches.

Using App Center

Searching apps
To search for an App, enter the keyword in the search bar.

Installing, updating, removing and migrating apps
To install an app, click the "+ Install" button. Then choose the volume to install the app to and the installation process will begin. After the installation process is complete, the "+ Install" button will change into the "O Open" button and you can click this button to launch the app. This app will then show up in "My Apps".

Note:
- The NAS must be connected to the Internet.
- If the NAS only has only one volume or the app does not support volume selection, you will not be prompted to choose a volume for app installation.
- QNAP is not responsible for troubleshooting any issues caused by open-source software/add-ons. Users are encouraged to visit the QNAP community forum or contact the software creators for assistance.
- When installing an add-on that requires a prerequisite app, the prerequisite add-on will be automatically added to the installation queue prior to the dependent add-on.
- If the app update process is canceled before it is finished, you must re-install the app from the App Center.
- When installing an app that requires higher system performance (such as Virtualization Station), it is recommended to install that app on a SSD.

To update a specific app, click "Update" under the app in App Center and then click "OK" to confirm. The button will turn to "Open" to signify that the update is complete. You can also click on the down arrow icon on the button to open an installed app; stop an app (the button will turn to "Start" after you stop an app, and you can click it to re-start the app); remove an app; migrate an app to a different volume; or add a shortcut to the app on the administrator's main menu, every user's main menu, or the login screen.

To update all apps at once, click "Update All" on the menu. Alternatively, to automatically update apps, go to the "App Center" > "Setting" > "Update", check "When updates are available, I want to", and select "Update Automatically." Click on "Apply" and "Close."

Note:
- Click the on/off button on an app icon to enable/disable an app.
- For more apps, please visit the QNAP official site (http://www.qnap.com/go/qpkg.html).
- Not all apps support app migration. For apps that do not support app migration, the option "Migrate to" will not be available when you click the down arrow icon below the app icon.

Offline Installation

To install apps when the NAS is offline or to install beta apps that are not officially available on the QNAP App Center, users can download the application (*.qpkg) from the QNAP website (http://www.qnap.com/go/qpkg.html) or forum (http://forum.qnap.com/), unzip the files, and click "Install Manually" on the menu bar to install the Apps manually.

DLNA Media Server

QNAP DLNA Media Server is developed by QNAP. To allow DLNA media players to access and play the NAS multimedia content via QNAP DLNA Media Server, enable the QNAP DLNA Media Server and configure the Media Library and the default user account.

> **Note:**
> - The contents allowed to be browsed on devices connected to the media server are based on the shared folder permission set for the default user account. Viewers can only watch multimedia contents from the media folders that the default user account is assigned the permission with. For media folder setup, please refer to the chapter on Multimedia Management. For permission assignment, please refer to the chapter on Shared Folder.
> - If you upload multimedia files to the default folder but the files are not shown in the Media Player, click "Rescan content directories" or "Restart server" on the DLNA Media Server configuration page.

Download Station

Download Station is a web-based download tool that allows you to download files from the Internet through BT, PT, Magnet Link, HTTP/HTTPS, FTP/FTPS, Xunlei, FlashGet, qqdl, Baidu Cloud downloads and RSS feed subscriptions. With the BT Search function, you can easily find BT seeds to download and make your NAS a 24/7 download center.
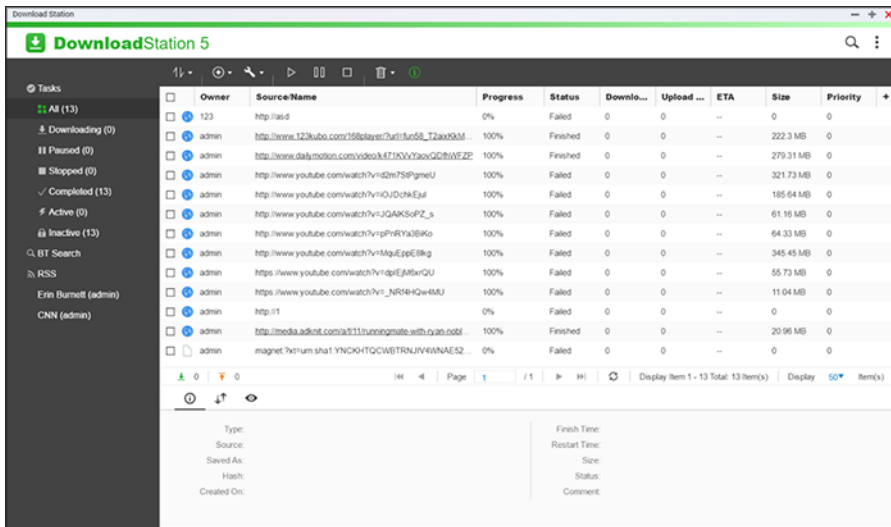
This chapter covers the following topics:

* Starting Download Station
* Familiarizing yourself with Download Station
* Download Station Settings
* Using Download Station

Important: **The Download Station is provided for downloading authorized files only.** Downloading or distributing unauthorized materials is against the law and may result in severe civil and criminal penalties. Users should be aware that they are subject to copyright restrictions and they will be held responsible for the consequences of their actions.

Note: For PT download, the supported client applications vary based on the PT sites. If the Download Station (libtorrent) is not in the client application list recommended by your PT sites, please search for an alternative one in the App Center.

Starting Download Station

Depending on your NAS model, Download Station may be enabled by default and can be launched from the Desktop or the Main Menu. If not, install and enable it from the App Center (for QTS 4.1 or later versions only.) Launch Download Station from the Main Menu/Desktop shortcut, or directly log into Download Station by going to: http://NAS_Name_or_IP/downloadstation/

Familiarizing yourself with Download Station

Menu Bar

No	Name	Description
1	Search	Click the magnifier button to show the search bar, type a keyword, and then click "Add-on" to select the search engine. Press enter to search for BT seeds. **Note:** The BT search feature is only available after you agree to the terms and conditions. Go to "Settings" > "Global" > " Search".
2	More	Click to display the following: • Settings - Configure BT or RSS settings (refer to the Download Station Settings section below). • Help - Open the Download Station Help. • About - Display information about Download Station.
3	View Mode and Task Filter	Click to select a view or to filter the task list.
4	Add download task(s)	Add a BT seed by entering the URL or upload a torrent file from the local PC.

5	Action	Start all, pause all, or pause all download tasks for a specified time period, remove all completed tasks, remove all completed tasks and delete data.
6	Start	Start BT tasks.
7	Pause	Pause BT tasks.
8	Stop	Stop BT tasks.
9	Remove	Click to remove BT tasks or to remove BT tasks and delete data.
10	Summary	Summary

Left Panel
- Tasks: List all BT tasks based on their download status (All, Downloading, Paused, Stopped, Completed, Active and Inactive.) Right-click on a task to start, pause, stop, remove, remove and delete data, or open the File Station folder..
- BT Search: Lists all BT seeds searched using the BT Search Bar. Right-click a searched BT seed to download that seed (create a task), open the link URL, or download the torrent file.
- RSS: List, add, edit, delete or update RSS feeds.

Download Station Settings

Go to "More" > "Settings" to configure Download Station.

Global Settings
- Download Schedule: Select continuous download or specify the download schedule. When setting the download schedule, select "Full speed" to use the global speed limit (unlimited) for all the download tasks. Select "Limited" to apply the speed limit settings of the downloaded services.
- Notification: Select to send a notification by email when a download task completes (SMTP settings must be configured properly in "System Settings" > "Notification".)
- Search: Agree to enable the BT search function.

HTTP
- Connection: Specify the maximum number of concurrent HTTP downloads.
- Bandwidth Limit: Specify the maximum download rate of HTTP download tasks. 0 means unlimited (the maximum number of concurrent HTTP downloads for x86-based NAS models is 30, and 10 for ARM-based NAS models.)

FTP
- Connection: Specify the maximum number of concurrent FTP downloads.

- Bandwidth Limit: Specify the maximum download rate of FTP download tasks. 0 means unlimited (the maximum number of concurrent FTP downloads for x86-based NAS models is 30, and 10 for ARM-based NAS models.)

BT

- Connection Setting:
  - Specify the ports for BT download. The default port numbers are 6881-6889.
  - Enable UPnP port mapping: Enable automatic port mapping on the UPnP supported gateway.
  - Enable DHT network: To allow the NAS to download the files even if torrent trackers cannot connect, enable Distributed Hash Table (DHT) network and specify the UDP port number for DHT.
  - Enable LSD network: To allow the NAS to discover local peers, enable local discovery service (LSD).
  - Enable NAT-PMP network: To automate port mapping and allow peers to easily download your files, enable NAT port mapping (NAT-PMP).
  - Protocol encryption: Enable this option for encrypted data transfer.
- Bandwidth Limit: Specify the maximum download rate of BT download tasks.
  - Global maximum concurrent downloads: Specify the maximum number of concurrent BT downloads (the maximum number of concurrent downloads for x86-based NAS models is 30, and 10 for ARM-based NAS models.)
  - Global maximum upload rate (KB/s): Enter the maximum upload rate for BT download. 0 means unlimited.
  - Global maximum download rate (KB/s): Enter the maximum download rate for BT download. 0 means unlimited.
  - Maximum upload rate per torrent (KB/s): Enter the maximum upload rate per torrent. 0 means unlimited.
  - Global maximum number of connections: The maximum number of allowed connections to the torrent.
  - Maximum number of connected peers per torrent: The maximum number of allowed peers to connect to a torrent.
- Seeding Preferences: Specify the share ratio for seeding a torrent and the sharing time. The share ratio is calculated by dividing the amount of uploaded data by the amount of downloaded data.
- Proxy: Specify the proxy server for BT download. Select the proxy type and enter the host IP and port, login username and password for the proxy server. For details on the setup of the proxy server, please refer to its user manual.
- BT Search: Select the BT engines to enable for BT search on the Download Station.

RSS

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

Add-on

You can enable and disable supported BT sites, torrent search engines and indexers on this page. New BT sites, search engines and indexers can be added as an Add-on to enrich the possibilities of Download Station.

> **Tip:** You can click the following link to download the developer guide for creating Download Station Add-ons: http://download.qnap.com/dev/download-station-addon-developers-guide_v4.pdf

File Hosting Account

You can save the login information for up to 64 HTTP and FTP accounts. To add login information, click "Add Account". Enter the host name or IP, username and password. To allow the login information to appear for account selection when configuring HTTP or FTP download, select "Enabled" next to the newly added account. To edit the settings of an account, select an entry on the list and click "Edit Account". To delete an account, select an entry on the list and click "Delete Account".

Using Download Station

Adding a download task

There are three ways to add download tasks:
1. Perform one of the following tasks.
    a. Drag and drop BT/PT files from the local PC to Download Station.
    b. Click "Add download task" (+) button and select Input URL or Torrent file.
    c. Search for BT files using the BT search function to add download tasks.
    d. Add an RSS feed and then create a download task.
2. Specify the following:
    a. Location of temporary files
    b. Location of completed downloads
3. Specify if you want to use your account credentials.
4. Click "Apply".

> **Note:**
> - The maximum number of concurrent downloads for x86-based NAS models is 60 (30 BT/PT and 30 HTTP/FTP) and 20 for ARM-based NAS models (10 BT/PT and 10 HTTP/FTP.)
> - Dragging & dropping BT files from PC to Download Station is only supported by Chrome and Firefox.

Adding HTTP, FTP, Magnet download tasks

1. Click "Add download task" (+) and select Input URL.

2. Enter the HTTP, FTP, or Magnet link. Note: Separate multiple entries by pressing "Enter". There should only be one URL on each line.

3. Click "Next".

4. Specify the following:

    a. Location of temporary files

    b. Location of completed downloads

5. Specify if you want to use your account credentials.

6. Click "Apply".

> **Note:** You can enter up to 30 entries at one time.

Managing downloads in a BT seed

You can right-click a task and select "Edit Downloads" to only select the files within a BT seed that you want to download.

Limiting the download/upload speed

To limit the bandwidth usage of the Download Station, configure the settings in "Settings" > "HTTP", "FTP", or "BT" > "Bandwidth Limit".

Scheduling downloads

To set scheduled downloads, go to "Settings" > "Global" > "Download Schedule". After enabling the download schedule, select "Full speed", "Turn off", or "Limited" and then click the preferred time slots.

Sending a notification after a download is completed

Go to "Settings" > "Global"> "Notification" and enable "Email".

Subscribing to and managing RSS feeds

You can subscribe to RSS feeds using the Download Station and download the files.

Adding an RSS subscription

1. Click "+" next to "RSS" on the left panel to add an RSS feed.

2. Enter the label.

3. Enter the feed URL.

4. Specify the following:

    a. Location of temporary files

    b. Location of completed downloads

5. Click "Apply".

6. Click "Close".

Downloading an RSS file

1. Select the file.
2. Perform one of the following tasks.
   a. Click "Add download task(s)".
   b. Right-click the file and select "Download".

The NAS automatically downloads the file. You can view the download status in the Downloading list.

Managing RSS subscriptions

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

Downloading torrent files using RSS Download Manager

You can use the RSS Download Manager to create and manage filters to download particular torrent files for BT Download.

- To add a filter, first launch the RSS Download Manager, select a label and click "Add".
- Enter the filter name and specify keywords to include and exclude.
- Select the RSS feed to apply the filter settings.
- You may also specify the quality of the video torrent files (leave it as "All" if you do not need this function or the torrent file is not a video.)
- Episode number: Select this option to specify particular episodes or a series of episodes. For example, to download episodes 1-26 of season 1 of a TV program, enter 1x1-26. To only download episode 1 of season 1, enter 1x1.
- Select the time interval for automatic update of RSS feeds. The NAS will update the RSS feeds and check if any new contents that match the filters are available.
- Click "Apply" to save the filter or "Cancel" to cancel or exit.
- To delete a filter, select the filter from the list and click "Delete".

Shortening BT seeding time

Go to "Settings" > "BT" > "Bandwidth Limit">"Seeding Preferences".
Change the "Share Ratio" to a smaller percentage or modify "Share Time" to shorten BT seeding time.

Sharing with multiple users

Administrators can grant Download Station access to NAS users, enabling friends and family members to enjoy the convenience brought by Download Station. Follow these steps to grant access to NAS users:

1. Go to "Control Panel" >"Privilege" > "Users"
2. Click the "Edit Application Privilege" button under "Action" for the user
3. Select Download Station.

4. Click "Apply".

Tips for slow BT download rates or download errors:

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

2. The NAS has been configured to use a fixed IP but the DNS server is not configured or it has failed.

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

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

   a. Manually open the BT port range on NAT router. Forward these ports to the LAN IP of the NAS.

   b. Recent 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.

Helpdesk

Helpdesk allows the NAS administrator to directly submit technical support requests or to suggest new features to our support team. For certain technical issues, a remote support session may be required. For these issues, you can enable a remote support session for our support team to directly solve your issues over the Internet.
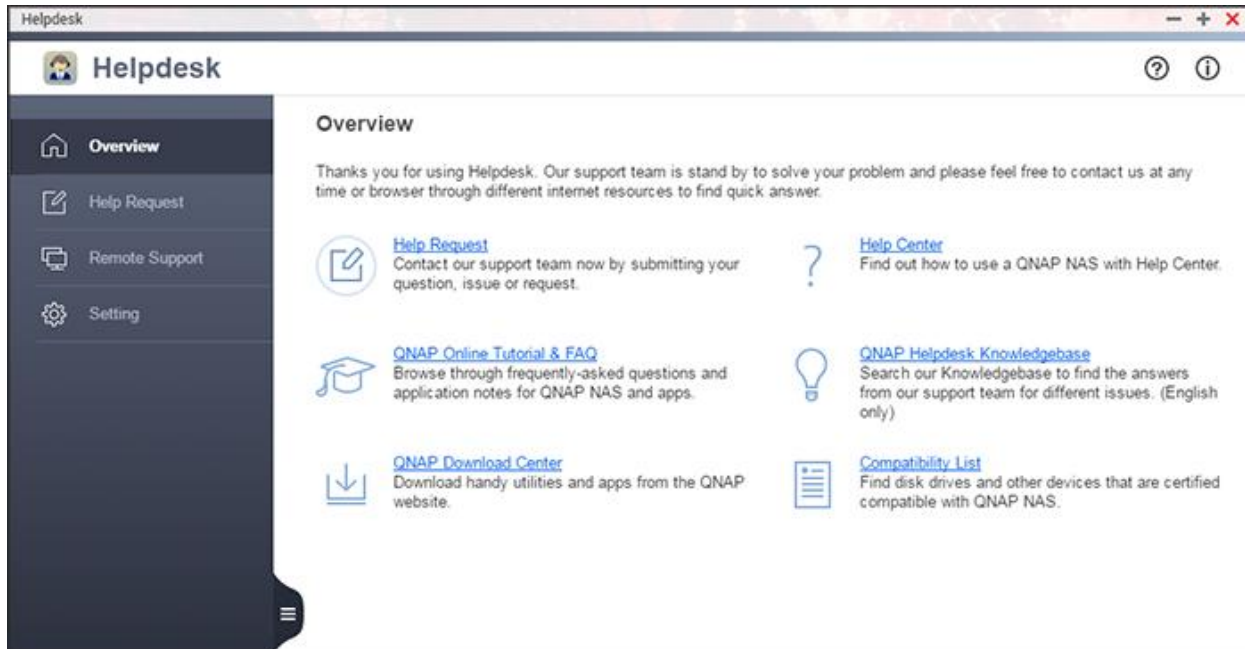
The general troubleshooting process with Helpdesk is as follows:
1. You submit a help request in Helpdesk.
2. The QNAP technical support team contacts you via email or phone to resolve your issues.
3. If a remote support session is required, the QNAP technical support team will notify you of relevant session details.
4. You enable Remote Support in Helpdesk using the Ticket ID.
5. The QNAP technical support team troubleshoots and resolves the reported issues.
6. If the issues cannot be resolved over the remote support session (one session is valid for 7 days), the QNAP support team will request an extension via email.
7. You extend the support session.
8. The QNAP technical support team notifies you that the issues have been resolved both in "Helpdesk" > "Remote Support" and via email.

In this chapter, the following topics are covered:
- Starting Helpdesk
- Submitting a help request
- Enabling remote support
- Configuring Helpdesk settings

Starting Helpdesk

Click the Helpdesk shortcut on the QTS desktop to launch it. If this shortcut is not available, please go to "App Center" and install and enable Helpdesk (for QTS 4.2.2 or newer). After enabling Helpdesk, you can also launch Helpdesk in "Desktop" > "More" > "Help" > "Help Center" > "Helpdesk".

Submitting a help request

Follow these steps to submit a help request from your NAS:
1. Ensure your NAS can reach the Internet.
2. Go to "Helpdesk" > "Help Request".
3. Fill out the ticket details. In the message field, please include the following information if possible:
   o Error message.
   o Time and date the error occurred.
   o The device, applications, and operating system that you used to access your NAS when the error occurred.
   o Steps to reproduce the error.
   o If the nature of your enquiry is product improvements or recommendations, please enter usage scenarios and similar products or functions and features in this field.
4. Choose to allow system logs to be sent to QNAP, upload other information such as the steps necessary to reproduce the error
5. Upload relevant screenshots or files.
6. Click "Submit".

The support team will contact you shortly with the email address you provided.

Enabling remote support

Following these steps to enable remote support:
1. Ensure your NAS can reach the Internet.
2. Go to "Helpdesk" > "Remote Support".
3. Enter the ticket ID and the email address you used for submitting that ticket.
4. Click "Enable Remote Support".

5. You must read and agree to the Terms of Service to use remote support.

6. Click "Confirm".

If the issues cannot be resolved over one remote support session, our technical support team will email you with a request to extend the support session. Please click "Extend a week" in the "Remote Support" page. After the issues are resolved, a message will be displayed on the "Remote Support" page and our technical support team will email you details regarding the reported issues.
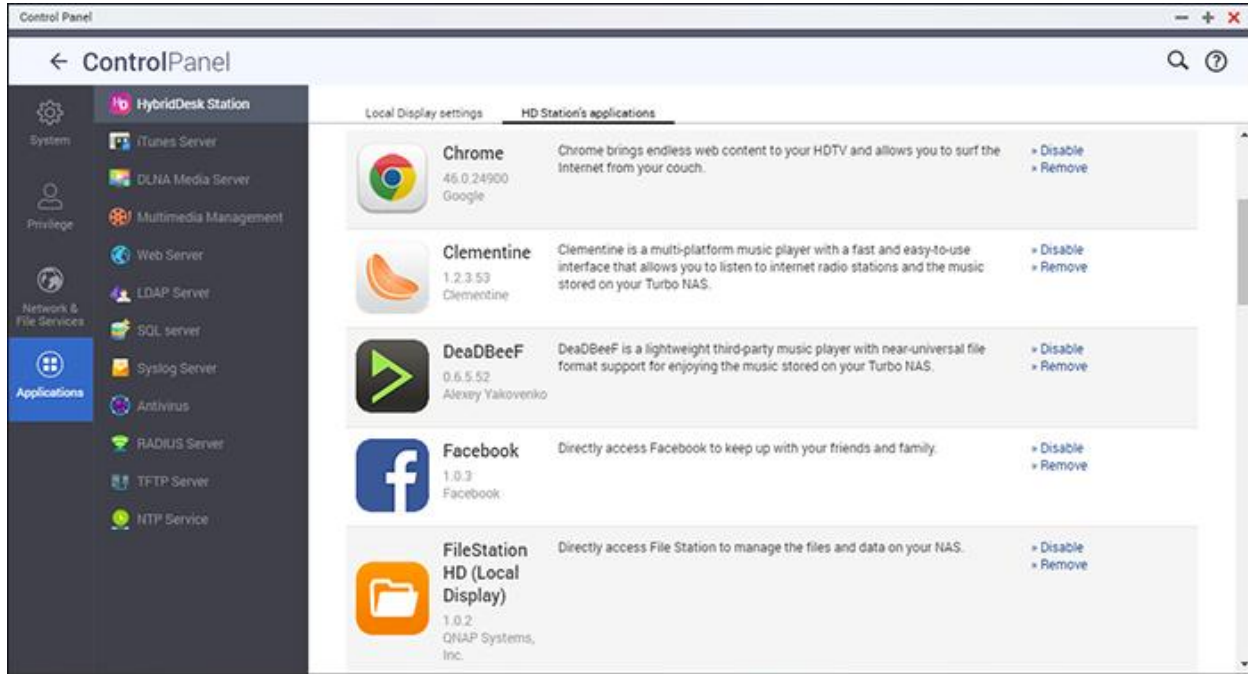
> **Note:**
> - One support session lasts 7 days starting from the time you click "Enable Remote Support".
> - Only the ticket specified by the QNAP support team can be used to enable Remote Support.
> - The helpdesk.qnap.com ports 22, 443 must be unblocked to allow our support team to connect to your NAS.
> - Before allowing our support team to connect to your NAS, it is recommended that you back up, move, or encrypt your data. To encrypt a shared folder, go to "Control Panel" > "Privilege Settings" > "Shared Folder" > "Edit Properties"

Configuring Helpdesk settings

You can configure the Helpdesk settings by going to "Helpdesk" > "Settings". The settings include your location and the option to allow system logs to be sent to QNAP.

HybridDesk Station

HybridDesk Station is a platform where numerous home and office apps can be installed to enhance your entertainment and productivity needs.

This chapter covers the following topics:

- Setting up HybridDesk Station
- Using HybridDesk Station
- Configuring HybridDesk Station

Note: To check whether your model support HD Station, go to http://www.qnap.com and use "HD station" as a keyword to find the related information.

Setting up HybridDesk Station

Create your lovely media environment by following these steps:

1. **Setting up the environment of the HybridDesk Station: Connect the NAS to the HDMI TV with a HDMI cable**
   - Remote controller: There are 4 different ways to control the HybridDesk Station.
     - QNAP remote controller
     - USB keyboard or mouse
     - Qremote: QNAP remote app, designed exclusively for the HybridDesk Station.

> **Note:** If you want to use Chrome on HD Station, you must use the Qremote mouse function or use a USB mouse that is connected to the NAS.

2. **Installing the HybridDesk Station**
   - Go to "Applications" > "HybridDesk Station" and click the "Get Started Now" button. The system will automatically install the HybridDesk Station.

3. **Choosing the applications to install**
   - You can choose from a variety of powerful QNAP and third-party applications to increase your work productivity and enrich your entertainment experience.

> **Note:**
> - Using Chrome or other applications may affect the hard drive hibernation of the NAS. Remember to exit the application and return to the HybridDesk Station portal.
> - To exit an application, press the power button on the remote control for 6 seconds at any time.
> - Press the one touch copy button on the NAS for 6 seconds to restart the HybridDesk Station.
> - For the best HybridDesk Station experience, we recommend using a NAS with at least 2GB memory.
> - The HybridDesk Station will restart when formatting an USB external device.

After installation, choose your preferred language on the TV screen, then you will see the HybridDesk Station portal.

4. **Enjoying HybridDesk Station: On the HybridDesk Station portal, select the application you want to use and start enjoying the service.**

Enjoy the comfort of your living room and play movies, photos, and music directly on your TV.

Using HybridDesk Station

Taking Pictures with Smart Phone and Watching them on TV
The first part is done by Qfile on your phone:
1. Use Qfile to browse your NAS.
2. Choose the multimedia shared folder.
3. Select the upload function.
4. Take a picture and upload it to the NAS.

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

5. Turn on your TV and choose HD Player.
6. Choose "Pictures".
7. Select the "Multimedia" folder.
8. Double click the picture you just uploaded.

Viewing Photos on your USB Device or Camera

Steps:

1. Connect a USB device or camera to the NAS.
2. Choose "Pictures".
3. Choose "Options".
4. Select the photo you want to view.

Configuring HybridDesk Station

Configure the HybridDesk Station by choosing "Settings" at the HybridDesk Station portal and HybridDesk Station in QTS.
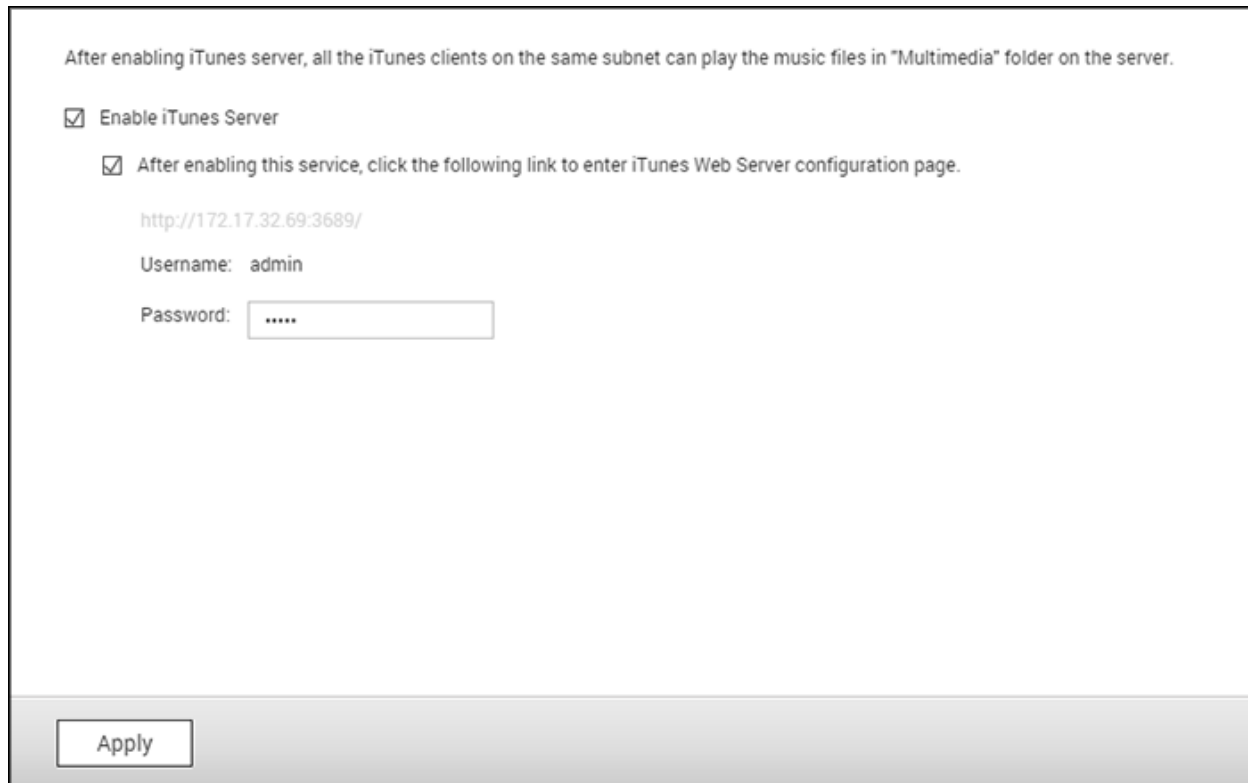
- HybridDesk Station portal:
  - App: Applications can be enabled or disabled here.
  - Display: Change the screen resolution and set up to turn off the screen after an amount of idle time.
  - Preferences: Here you may change the language or type of remote control and audio output. The default setting is HDMI. If there is an installed USB sound card, you can choose that option in the NAS Audio Output.
- HybridDesk Station in QTS:
  - Output resolution: Change the resolution for the HybridDesk Station portal screen. Before you change this setting, please make sure that no apps are opened in the HybridDesk Station portal.
  - Overscan: This setting can reduce the visible area of a video displayed on the HybridDesk Station portal. The higher the percentage, the more the visible area will be reduced.

> **Note:**
> - Only the QNAP remote or MCE remote control is supported. NOT all of the TS-x69 models support the internal remote control and the TS-x70 models only support the MCE remote control.
> - HDMI Audio Passthrough is currently not supported by the TS-x69 series.

iTunes Server

Using this service MP3 files in the Qmultimedia/Multimedia folder of the NAS can be shared with iTunes. Computers on the LAN with iTunes installed will be able to find, browse, and play the shared music files.

To use the iTunes Server, enable this feature and then upload music files to the Qmultimedia/Multimedia folder of the NAS.

Note: iTunes Server may be disabled or hidden on some Enterprise and SMB models. To enable iTunes server, please refer to "System Administration" in the General Settings section.

To configure the iTunes server settings and add smart playlists, login to the iTunes server web page (http://NAS-IP:3689/index.html.) Connect the PC and the NAS to the same LAN and run iTunes on the PC. Find the NAS name under "SHARED" and music and playlists will be available.

Additional Reference:
- Setup iTunes Music Server on QNAP.

Multimedia Management

Media Library scans photos, music, and videos from designated media folders and indexes them for multimedia applications. Thumbnails for media files will be generated to enhance your user experience as you browse through them in their corresponding applications. You can configure multimedia settings in "Control Panel" > "Applications" > "Multimedia Management".
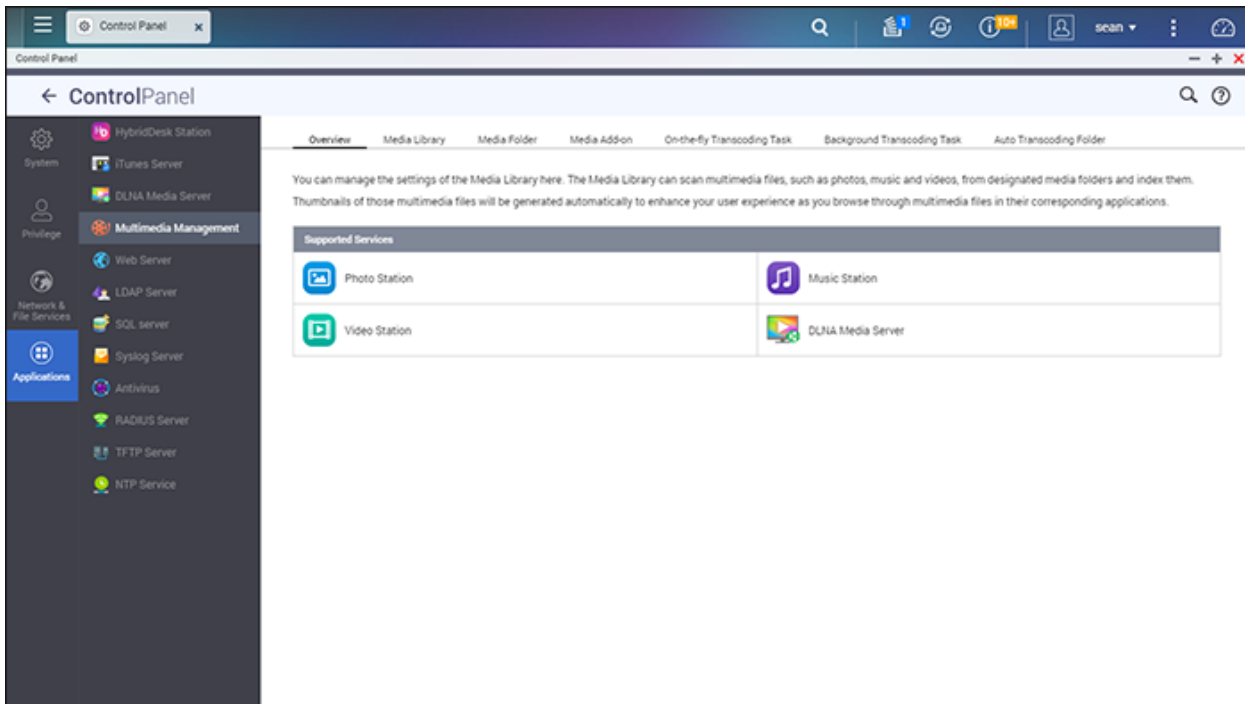
Media Library

- Scan Setting: Three options are provided for the media scan:
  - Real-time scan: New files are scanned as soon as they are added to media folders.
  - Scan by schedule: Specify a start and end time for the scan, and it will be automatically conducted on a daily basis.
  - Manual Scan: You must click "Scan now" to check for new media.
- Set media scanning priority to high: The option will allow the Media Library to immediately process media files in order to quickly generate thumbnails. When the NAS needs to run scan tasks and transfer files at the same time, it will lower the file transfer speed and prioritize media scan tasks.
- Multimedia code page setting: Change this setting to the corresponding code for non-UTF media files for fonts and characters in the associated applications to be displayed correctly.

- Rebuild media library indexing: By rebuilding the media library, the NAS will scan the specified media folders and replace the existing library with a new one.

You can enable or disable Media Library by clicking "Activate Media Library" or "Deactivate Media Library". Please note that disabling Media Library will make multimedia applications function incorrectly. For more information, see the notes below.

> **Note:**
> - If Media Library is disabled, multimedia services such as Photo Station, Music Station, DLNA Media Server, and OceanKTV will function incorrectly.
> - By default, image files with a width or height less than 400 pixels will not be indexed and will not have any thumbnails generated. Nevertheless, you can this setting and set up the minimum image size to index in "Control Panel" > "Applications" > "Multimedia Management" > "Media Folder" > "Setting".

Media Folder

Media folders are shared folders on the NAS that are scanned for multimedia files. "/Multimedia" and "/Home" are the default media folders on the NAS (from QTS 4.1, all default shared folders on the NAS are identified as media folders for the purpose of multimedia application services.) To add media folders: click "Add", select media types and folders from the list, and click "Add". To change scanned file types for the media folders, first uncheck the media file types and click "Apply". To remove media folders, first select media folders from the list, and then click "Delete" and "Apply".

Transcode Management

Transcoding is the process of converting video files into an universal format (*.MP4) that is compatible with most media players, including mobile devices and Smart TVs. Converted files with a range of resolutions can be used across different network environments for better viewing experience. After transcoding tasks are created, they can be managed here. This service is enabled by default.
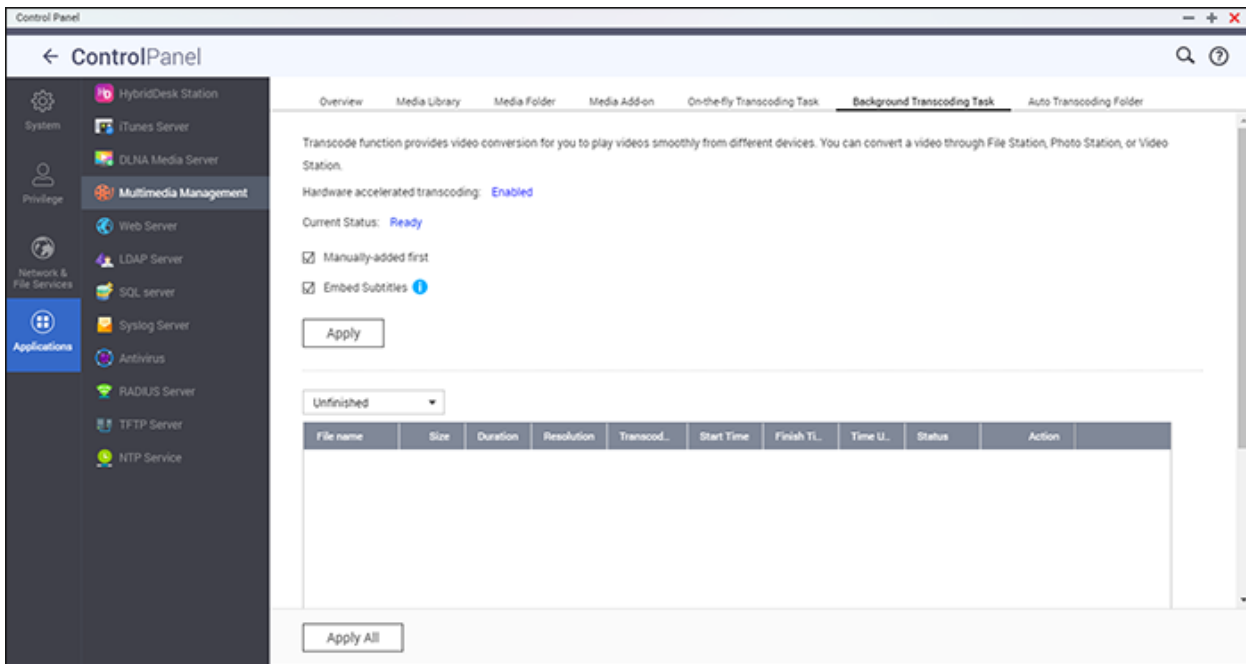
On-the-fly Transcoding Task

On-the-fly transcoding will simultaneously convert and stream a video while you watch it. This task requires some computing resources. If your NAS has hardware transcoding acceleration, it is recommended to install CodexPack to accelerate transcoding and reduce CPU usage. You can monitor and manage the use of on-the-fly transcoding services.

Manage transcoding tasks using the following buttons:

Button	Name	Description
Refresh	Refresh	Refresh the list.

Manage each task with the following buttons:

Button	Name	Description
	Priority	Adjust the order each task is executed.
	Remove	Remove the selected task from the list.

Note: This feature is for the x86 series NAS only. Please check the product page (software specification) on the QNAP website (www.qnap.com) to see if this feature is available for your model.

Background Transcoding Task

Background transcoding is when a video file is converted in advance, potentially avoiding high CPU usage if the video will be simultaneously accessed by many users. You can manually add videos to be transcoded using File Station, Photo Station, or Video Station. Video files can be converted to 240p, 360p, 480p, 720p and 1080p and will be saved in the "@Transcode" folder that is in the same directory as the video.

Manage all transcoding tasks using the following buttons:

| Button	Name	Description
Stop Transcoding	Stop Transcoding	Suspend all ongoing tasks in the list.
Remove All Incomplete Tasks	Remove All Incomplete Tasks	Remove all tasks that are yet to finish from the list.
Remove All Complete Tasks	Remove All Complete Tasks	Remove all complete tasks from the list.
Refresh	Refresh	Refresh the list.

Manage each task with the following buttons:

Button	Name	Description
	Priority	Adjust the order each task is executed.
	Remove	Remove the selected task from the list.

Auto Transcoding Folder

This feature is designed to convert the contents of an entire folder, and within the folder, the resolution of each subfolder can be specified independently. Click "Add" to add a new folder and select the video quality (resolution) and the folder to add it to the task list.

Music Station

Music Station (5.0) helps you create a personal music center on the cloud. This web-based application is designed for users to play music files on the NAS, listen to thousands of radio stations on the Internet, and share your music with your friends and family. Your music collection stored on the NAS is automatically organized into categories for easy access.
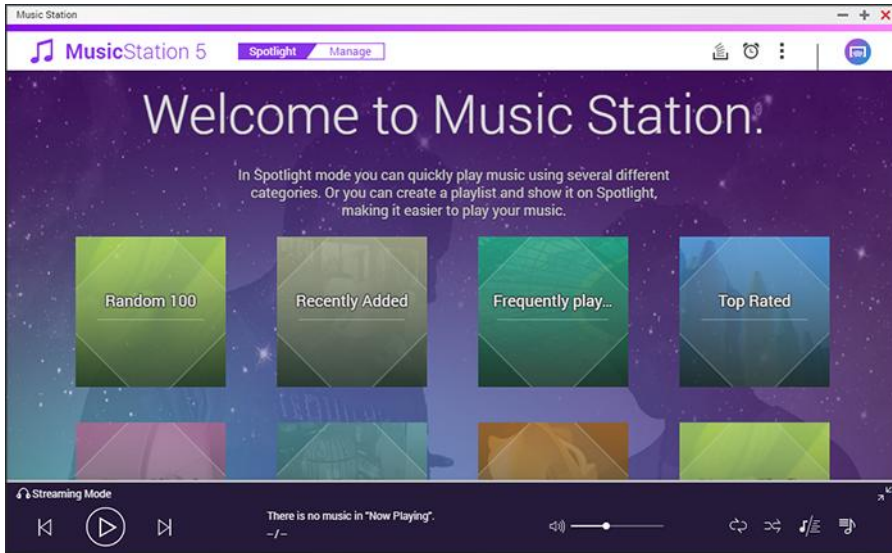
This chapter covers the following topics:

- Starting Music Station
- Familiarizing yourself with Music Station
- Using Music Station
- Media Library and Privacy Settings

Starting Music Station

Depending on your NAS model, Music Station may be enabled by default and can be launched from the Desktop or the Main Menu. If not, install and enable it in the App Center (for QTS 4.1 or newer versions only) and follow these steps:

1. Upload music files to a shared folder on the NAS. There are three ways to upload music files to the NAS: 1) Install Qfinder Pro on your PC or Mac, set up a network drive and upload files to your preferred shared folders. For details on setting up a network drive, please check the Connecting to NAS Shared Folders chapter; 2) In Manage Mode, click "Import Music" (up arrow) on the menu bar or drag & drop files to the Music Station window. In the "Upload" window, select the destination folder and then either click "Select the music file to upload" or drag & drop files to the dotted rectangle to upload files. 3) Click "Folder" on the left panel, open the folder where you want to upload files, and drag & and drop music files here.
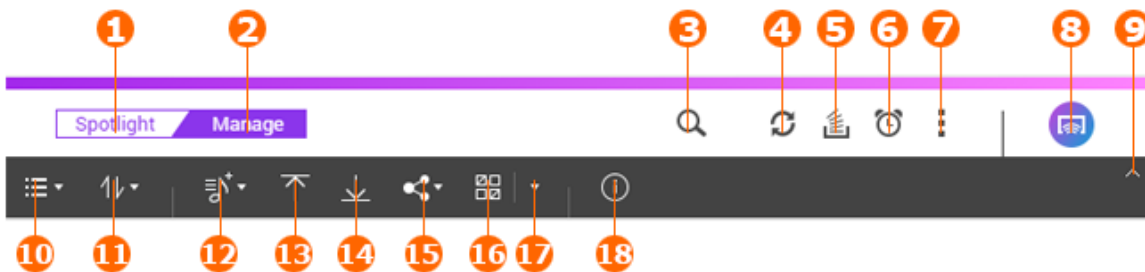
2. Launch Music Station from the Main Menu/Desktop shortcut, or directly log into Music Station by going to: http://NAS_Name_or_IP/musicstation/

Familiarizing yourself with Music Station

Menu Bar

No	Name	Description
1	Spotlight Mode	Provide an intuitive interface for you to view and play songs in default categories and your own playlists.
2	Manage Mode	Provides a detailed interface for you to manage and share your music files.
3	Advanced Search	Search songs by their title, artist, rating, and other information.
4	Refresh	Refresh the current page.
5	Background Task	Shows tasks running in the background, such as uploading.
6	Music Alarm	Set music alarms.
7	Settings	Provides more setting options and shows Help, Quick Start, and About.
8	Multi-zone Control and Streaming	Streams music to the devices on your network and manage Now-playing lists on each device.
9	Show/Hide Menu	Show or hide the lower part of the menu.

	Bar	
10	Items Viewing	Show items in List Mode or Thumbnail Mode
11	Sort	Sort items by various attributes in ascending or descending order.
12	Add Playlist	Create a playlist or a smart playlist.
13	Import Music	Upload music files from your local device.
14	Download	Download music files to your local device.
15	Share Music	• Share link via email: Please ensure that your email settings are correctly configured. Click your profile icon in the top-right corner of the desktop and go to "E-mail Account" to set up your account. You can also specify the subject and add a message to the mail. • Share link on social networking websites: Choose your preferred website and add a message to supplement your link. • Create link code: Select a domain name and format for the link of your music files or playlists • For all three methods, you can decide whether to protect files with a password, allow users to download files, and you can also choose an expiration date for your sharing. After you share music files, you can view and re-share them in "Shared Center".
16	Multi-Select	Select multiple items.
17	Select/Deselect All	Select or deselect all the items.
18	Information	View and modify the information of the selected item.

Player

No	Name	Description
1	Progress Bar	Control the playback progress.
2	Mini Player	Minimize the player (not available if you choose "Tab Mode" in

		"Desktop Preferences").
3	Previous	Play the previous song.
4	Play/Pause	Play or pause the current song.
5	Next	Play the next song.
6	Volume	Adjust the volume.
7	Repeat	Repeat the current song or repeat all the songs in the playlist.
8	Shuffle	Randomly play songs in the playlist.
9	Lyrics	Show the lyrics of the current song.
10	Now Playing	Show the Now-playing panel. Drag & drop songs to the panel to add them to the now-playing list.

Note:

- To stream media files to HDMI or Chromecast using the Network Media Player, Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".

Left Panel

- Songs, Artist, Album, and Genre: All authorized music files are listed and grouped into these four categories.
- Private Collection: Personal music files in the "/home" folder are listed here. These music files belong to the user that is currently logged in.
- Qsync: Music files synchronized with the Qsync service are listed here.
- Folder: You can view and manage the music files in media folders here.
- Playlist: You can create, manage, and delete playlists here. Each playlist can include up to 600 items, and Music Station can contain up to 200 playlists.
- Smart Playlist: You can create smart playlists that only include songs meeting your own criteria.
- Shared Center: Your shared music files are listed here. You can view their sharing history and share them again.
- My Favorite Radio: Enter the radio URL or search TuneIn Radio to add your favorite radio stations on the Internet (up to 1024 stations). Please note that only the URLs with the MP3 format are supported.
- TuneIn: Users can browse and play on-line radio stations streamed by TuneIn.
- Trash Can: All deleted music files can be found here. You can either restore or permanently delete them.

Using Music Station

Import music files

Please refer to the Starting Music Station section.

Creating and managing playlists

To create a playlist, click "Add Playlist" on the menu bar and select "Create a Playlist," or drag & drop music files onto "Playlist" on the left panel. You can also create a Smart Playlist that only contains songs meeting your criteria. To share a playlist, select a playlist and click "Create a new share" on the menu bar to email it to other people, publish it to social networking sites, or create a link for it. After you share playlists, you can view the detailed information about your shared lists in "Shared Center". You can also right click a playlist and add it to the "Now Playing" list or select "Information" to change its name or modify its settings.

Sharing playlists

When you create a playlist, you have to decide how to share it with other NAS users. You can choose to make it open to all the NAS users or just the creator and administrator (and allow them to edit it), or you can choose not to share it at all by leaving both options unchecked.

You can also share a list of songs as you do with playlists. To do so, click "Songs" on the right panel, select songs from the list, and click "Create a new share" to choose the way you want to share the list. Please note that the difference between a playlist and a list of songs is that the former falls into the "Playlist" category on the left panel, while the latter is a temporary list of songs selected from different albums.

Multi-zone control and streaming

Music Station works with your NAS Audio output (USB speaker, Soundcard, HDMI), Bluetooth, SONOS devices, and Network Media Players (DLNA, Chromecast, AirPlay), making it easy for you to stream music to many types of devices. It can stream different music to all the supported devices in your home or play the same music at the same time. You can change the output devices by clicking the purple button in the top-right corner, drag and drop songs to the Now Playing list on your desired devices, and then double click a song to play it.

Changing album covers or artist photos

Music Station automatically searches for an image for your albums and artists. If an appropriate cover cannot be found, you can also import your own images. To change album covers or artist photos, follow these steps:

1. Select "Album" or "Artist" on the left panel.
2. Right click an album or an artist and select "Information". In the information window, click the album cover or artist photo to upload your own images. You can also click "Search" to search for images on the Internet.

Finding your music files quickly

To quickly locate your music files, you can rate or classify them:

- You can either select a file and click "Information" on the menu bar or right click a file and select "Information". You can then give it a rating or modify its data in the information window.
- To rate or modify music multiple files, click the multi-select button on the Main Menu (or hold the Ctrl key) and select your desired files to rate and modify them all at once.

After music files are rated or classified, they can be searched by their rating, artist, genre, or other attributes in Advanced Search.

Media Library and Privacy Settings

Music files in Music Station are listed and displayed according to shared folder privileges (media folders) and settings in Media Library. For shared folder privileges, only users (including domain users) with the permission to access a shared folder can view its contents in Music Station. For example, if a user does not have read/write or read-only permissions to access a shared folder, that user cannot see the music files in the shared folder. The administrator can give or deny other users permissions to access various functions in Music Station. To configure privilege settings, click "More settings" in the top-right corner and go to "Access Permissions".

Note:
- Besides shared folder privileges, you can also import your private music files to your "/home" shared folder to hide them from other NAS users (except the NAS

administrator.) Your "/home" folder contents can be found under "Private Collection".

- To create a shared folder, go to "Control Panel" > "Privilege Settings" > "Shared Folders".

Music files stored in the shared folders are only visible after they are detected and scanned by Media Library. To set Media Library to scan for music files manually or by a schedule, go to "Control Panel" > "Multimedia Management" > "Media Library". For more information about media folder settings, please refer to the chapter on Multimedia Management.

Note: Because the media folders in Media Library are shared by Photo Station, Music Station, Video Station and DLNA Media Server as their content source, content will be affected in those applications if new media folders are added or existing media folders are removed from Media Library.