QNAP ES NAS

Software User Manual

(Version: 1.1.x)

This manual is applicable to the following ES (Enterprise Storage) NAS models: ES1640dc, ES1640dc v2, TES-1885U, TES-3085U.

*Unless otherwise specified, the content of this manual applies to all the above NAS models.
*The screenshots in this manual are for reference only, as their content may differ by model.
*For user manuals of other NAS models and firmware versions, please visit http://docs.qnap.com.

Published: 10/05/18

Table of Contents

Notice

- Legal Notice and Disclaimer
- Regulatory Notice
- Document Annotation
- Safety Information and Precautions

Legal Notice and Disclaimer

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

- The ES NAS is hereafter referred to as the NAS.
- This manual describes the features and functions of the NAS. The product you purchased may not support certain features which are model-specific.

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, lifesaving, 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 ES NAS models comply with different CE compliance classes. Please refer to the table for details.

FCC	CE	ES NAS Models
Class A	Class A	ES1640dc, ES1640dc v2, TES-1885U, TES-3085U

Document Annotation

Annotations in this document

- ***Warning:*** The instructions must be strictly followed. Failure to do so could result in injury or death.
- ***Caution:*** 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:*** 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:

1. Hardware Installation
2. Software Installation
3. Getting Utilities
4. Connecting to the Shared Folders
   - Windows
   - Mac or FreeBSD
5. Connecting to the NAS by Web Browser

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. Check the compatibility list on the QNAP website (http://www.qnap.com/compatibility) for 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. Check the hardware user manual for more details.

Note:

- For the ES NAS series, the first four HDD bays on the front are reserved for system partitions. For TES NAS models, the first four HDD bays on the front or the first four HDD bays on the rear are reserved for system partitions. HDD bays that are reserved for system partitions are marked with a sticker on the HDD tray.
- The information is also illustrated in the Quick Installation Guide (QIG) that can be found in the product package or at http://start.qnap.com.
- If you encounter a "Device not found" message, ensure that:
  - Your NAS has been powered on.
  - The network cable is connected to the NAS.
  - The orange and green indicator lights on its LAN port(s) are blinking.

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.

Software Installation

After installing the NAS hardware, proceed to software installation with these steps:

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 "Qfinder Pro Utility Installation".
5. Choose your operating system, then download and install Qfinder Pro.
6. Run Qfinder Pro and let it 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 QES with your QES account username and password to log in (QES is the operating system for the ES NAS.)

Getting Utilities

QNAP has prepared a number of practical and useful utilities to enhance your NAS experience. To download them, open http://www.qnap.com and go to "Support" > "Download". Specify your NAS mode, and then click "Utility" for a full list of utilities that are compatible with your NAS.

Connecting to Shared Folders

After configuring networking, storage pools, and shared folders in QES, it is time to connect to the shared folders on the NAS. Refer to these links for the connection setup:

Windows

1. Open 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 (Ethernet interface).
2. Enter the default administrator name and password. The default login ID and password are both "admin".
3. Upload files to the shared folders.

Note: Each controller has two kinds of network interfaces: management interface and Ethernet interface (dedicated for data transfer). The NAS_IP in the Step 1 above refers to either of the Ethernet interfaces on the controller.

Mac, Linux or FreeBSD

Mac Users

1. Choose "Go" > "Connect to Server".
2. Enter the NAS_IP (Ethernet interface).
3. Enter your login ID and password.

4. Select the folder you want to mount and click "OK".
5. The folder is mounted.

Linux or FreeBSD

On FreeBSD, run the following command:

```
mount -t nfs <NAS IP(Ethernet interface)>:/share/<Shared Folder Name> <Directory to Mount>
```

For example, if the IP address of the NAS is 192.168.0.42 (Ethernet interface), to connect to a shared folder "public" under the /mnt/pub directory, use the following command:

```
mount -t nfs 192.168.0.42:/share/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.
- Each controller has two kinds of network interfaces: management interface and Ethernet interface (dedicated for data transfer). The NAS IP in the example above refers to either of the Ethernet interfaces on the controller.

Connecting to the NAS by Web Browser

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

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

Note:

- Each controller has two kinds of network interfaces: management interface and Ethernet interface (dedicated for data transfer). The NAS IP in the example above refers to the management interface.
- The default IP for the management interface on Controller A is 169.254.100.100:8080 while for Controller B, the IP for the management interface is 169.254.100.101. If the NAS has been configured to use DHCP, you can use QNAP Qfinder Pro to check the management interface 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.
- Accessing the NAS from a Microsoft Internet Explorer 10 browser may result to a blue screen. To resolve this issue, users must enable active scripting. Go to “Tools” > “Internet Options” > “Security” > “"Custom level...". On the “Security Settings - Internet Zone” window, go to "Scripting" > "Active scripting" and then select "Enable".

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: Secure login uses port 443. To securely log into the NAS via the internet, ensure port 443 is open and forwarded to the NAS on your NAT router or firewall.

3. The NAS Desktop will be displayed.

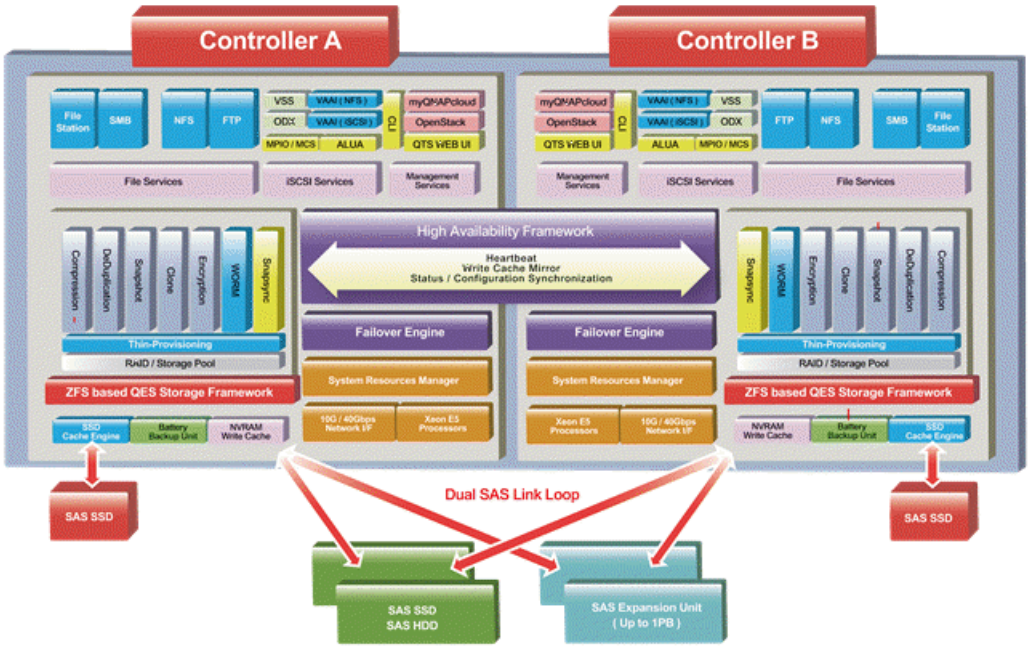
QES Basics and Desktop

QES 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 QES:

- Introducing QES
- Using QES Desktop

Introducing QES

The QES (QNAP Enterprise System) operating system is based on FreeBSD Kernel and ZFS to provide the stability and functionality of traditional Linux operating systems and native file systems.



QES is designed and optimized for the following features:

- Remote data synchronization: Block-level SnapSync provides remote backup and disaster recovery at any time.
- Application consistent snapshots: Snapshot Agent provides data consistency when taking snapshots.
- Higher-capacity efficiency: Block-level deduplication, real-time data compression, and thin provisioning.
- High availability, high reliability, and high serviceability: Supports dual active controllers, dual Mini-SAS channel backup and can tolerate single node failure to ensure uninterrupted mission-critical enterprise tasks and productivity.

- Minimal backup configuration: When creating a QNAP Snapshot Agent and VSS Hardware Provider operating environment, all applications, including VSS Service, Requestor, Provider and QNAP Snapshot Agent, can be deployed with VSS-Aware applications on the same server. The minimum requirements are one QNAP ES NAS and one server.
- Excellent random write performance: Battery-protected DRAM write featuring cache data protection coupled with Flash read acceleration provides industry-leading performance.
- Well-rounded networking support: A single system supports 10 Gigabit Ethernet and iSCSI, providing excellent storage deployment flexibility.

Note: The "high availability" and "battery-protected DRAM write-cache" features are only available on dual controller ES series NAS.

Using QES 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.

NO.	Name	Description
1	Main Menu	Show the Main Menu. It includes two parts: 1. QNAP applications (APPLICATIONS): Applications developed by QNAP to enhance your NAS experience, such as File Station. 2. System features and settings (SYSTEMS): Key system features designed to manage or optimize your NAS;
2	Show Desktop	Minimizes/restores all open windows.
3	myQNAPcloud	Go to the myQNAPcloud website.
4	Background Task	View, pause or stop tasks running in the background. Examples of background tasks are HDD SMART scan and file backup.
5	External Device	List all external storage devices that are connected to the NAS via its Mini-SAS ports. Click the "External Device" header to open the External Device page for relevant settings and operations. Please note that the ES NAS currently only supports JBODs connected via SAS cable, and UPS connected via SNMP. For details, see External Device.
6	Event Notifications	Check for recent system error and warning notifications. Click "Clear All" to clear the list. To review all historical event notifications, click the "Event Notifications" header to open the System Logs. For details on System Logs, refer to the System Logs chapter.

7	Options	• Profile: Specify your email address and change your profile picture. You can also view connection logs and edit the login screen here. • Wallpaper: Change the default wallpaper or upload your own wallpaper. • Change Password: Change your login password. Length must be 5 to 64 characters. • Miscellaneous: o Auto logout after an idle period of: Specify the idle period before the current user is automatically logged out. This option is by default enabled, with an auto-logout time of one hour. o Warn me when leaving QES: Users will be prompted for confirmation each time they leave the QES Desktop. For example, when they click the browser back button or close the browser. It is advised to check this option. o Reopen windows when logging back into QES: Check this option, and all the current desktop settings (such as the "windows opened before your logout") will be kept after your next NAS login. o Show the desktop switching button: Check this option to hide the next desktop button (No. 14) and only display them when you move your mouse cursor close to the buttons. o Show the link bar on the desktop: Uncheck this option to hide the link bar. o Show the Dashboard button: Uncheck this option to hide the Dashboard button (NO. 15). o Show the NAS time on the desktop: Uncheck this option to not display the NAS time in the bottom-left of the desktop. o Keep Main Menu open after selection: When checked, the main menu does not auto-hide after a user opens it. It will remain open on the left-side of the desktop until a user closes it again.
	Admin Control	Customize user-specific settings, change your user password, restart/shut down the NAS or log out your user account. • Last login time: The time the system was last logged in. • Options: Refer to No. 7 above. • Change Password: Change your password. Length must be 5 to 64 characters. • Restart: Restart your NAS. Select “Restart the system without interrupting services" to ensure uninterrupted NAS services. For "Restart the system without interrupting services", the controller you are restarting will first takeover and the standby controller will reboot first. After the standby controller is powered up and ready, it will take over and

		return control back to its peer after the peer is ready. This process will take a long time to finish, but this option can ensure uninterrupted NAS services. • Shutdown: Shut down your NAS. ○ **Note: To power off a NAS, you can also run Qfinder Pro and click "Tools" > "Shut down Device".** • Logout: Log yourself out. • About: Check for the NAS model, firmware version, HDDs already installed and available (empty) bays.
9	Search	Enter a feature specific keyword in the search bar to search for the desired function and its corresponding help. Click the result in the search bar to launch the function or open its online QES help.
10	Online Resource	A list of available resources can be found here, including: • Quick Start • Virtualization Guide (a NAS user guide to virtualization) • QES Help • Tutorials • Wiki (A QNAP wiki containing user generated help topics) • Forum (learn from and interact with other QNAP users) • Customer Service (check for customer support resources) • Feedback (File a feature request and bug report)
11	Language	Choose your preferred language for the UI.
12	Desktop Preference	Choose the application icon display style and select your preferred application opening mode on the desktop. Application icons can be switched between small and detailed thumbnails. Applications can be opened in Tab Mode or Window Mode. Only Tab Mode is available if you log into the NAS using a mobile device. • Tab Mode: In this mode, the window will be opened 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 and reshaped to a desirable style.
13	Desktop Area	Remove or arrange all applications on the desktop, or drag one application icon over the top of another to put them in the same folder.
14	Next Desktop/ Last Desktop	Switch between desktops.
15	Dashboard	Check important NAS statistics, including system and HDD health, resources,

		storage usage, online users, scheduled tasks, etc. Click the header within each widget to open its respective page.

Tip:

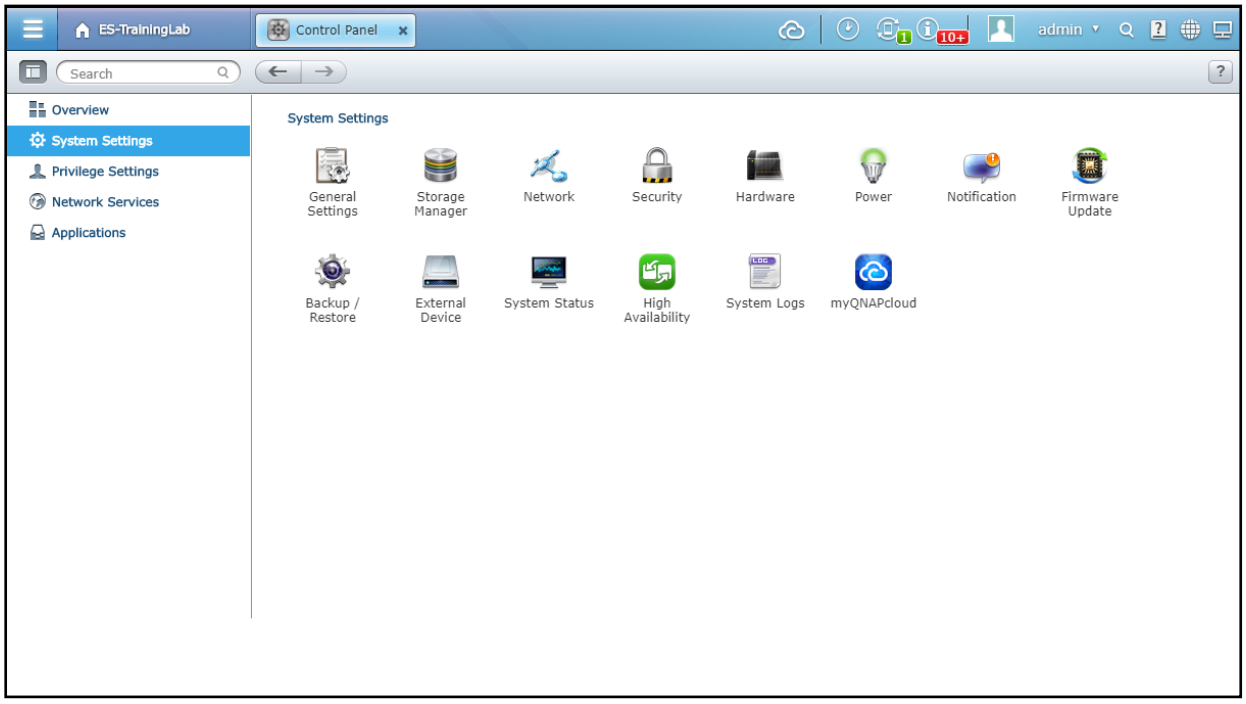
- All of the Dashboard widgets can be dragged onto the desktop for monitoring specific details.
- The Dashboard will be presented differently on different screen resolutions.
- The color of the Dashboard button will change based on the status of system health for quick recognition.

Note:

- The minimum recommended screen resolution for QES is 1280x800.

System Settings

Go to "Control Panel" > "System Settings" to set up your NAS.

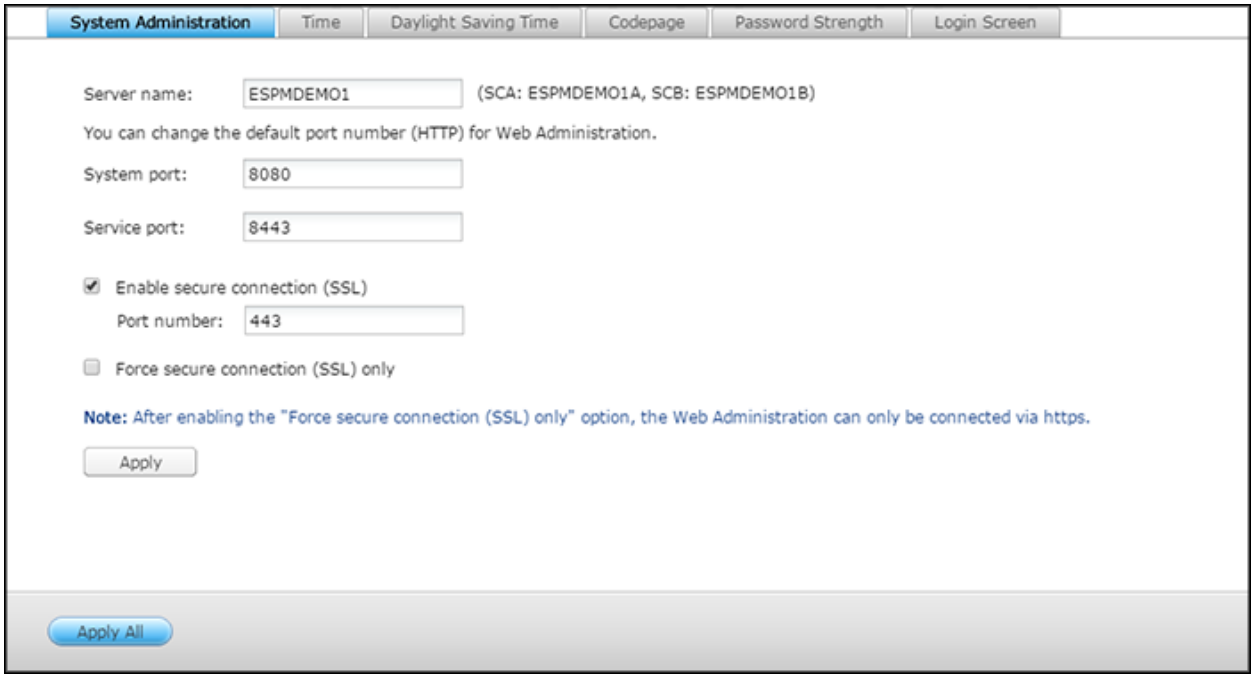


For details on the settings, refer to the following links:

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

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
- Password Strength
- Login Screen

System Administration

- Server name: Enter the name of the NAS. The NAS name supports a maximum of 14 characters and can be a combination of letters (a-z, A-Z), numbers (0-9), and dash (-). Space ( ), period (.), and a name consisting of only numbers are not allowed.
- System port: Enter the port number for system management using the web interface. The default port is 8080.
- Service port: This port can be used by services and utilities, such as the QNAP SRA plug-in for VMware.
- Enable Secure Connection (SSL): Allows users to connect to the NAS by HTTPS. Enable secure connection (SSL) and enter the port number.

Time

Adjust the date and time format and time zone according to the location of the NAS. If the time on your NAS is 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 in the event logs will be inconsistent with the actual time when an action occurs.
- Scheduled jobs will be run at the wrong time.

- Time zone: Select your NAS time zone, according to location.
- Date and time format: Select how the date will look, and choose between a 12 hour or 24 hour clock.
- Manual Setting: Manually set the time of the NAS.
- Synchronize with an Internet time server automatically: 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: Click "Update" to synchronize the time of the NAS with your computer's time.

Note: First time synchronization may a few 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.

Password Strength

Enable password policy rules forces NAS users to set stronger, more secure passwords. You can enable one or more of the following rules:

• The password must contain characters from 3 of the following 4 types: Lowercase [a-z], Uppercase [A-Z], Numeric [0-9], Special Characters such as [!@#$%..]

• No character may be repeated 3 or more times consecutively. For example: AAA.

• The password must not be the same as the username, or username reversed. For example, Username:user1, password:1resu.

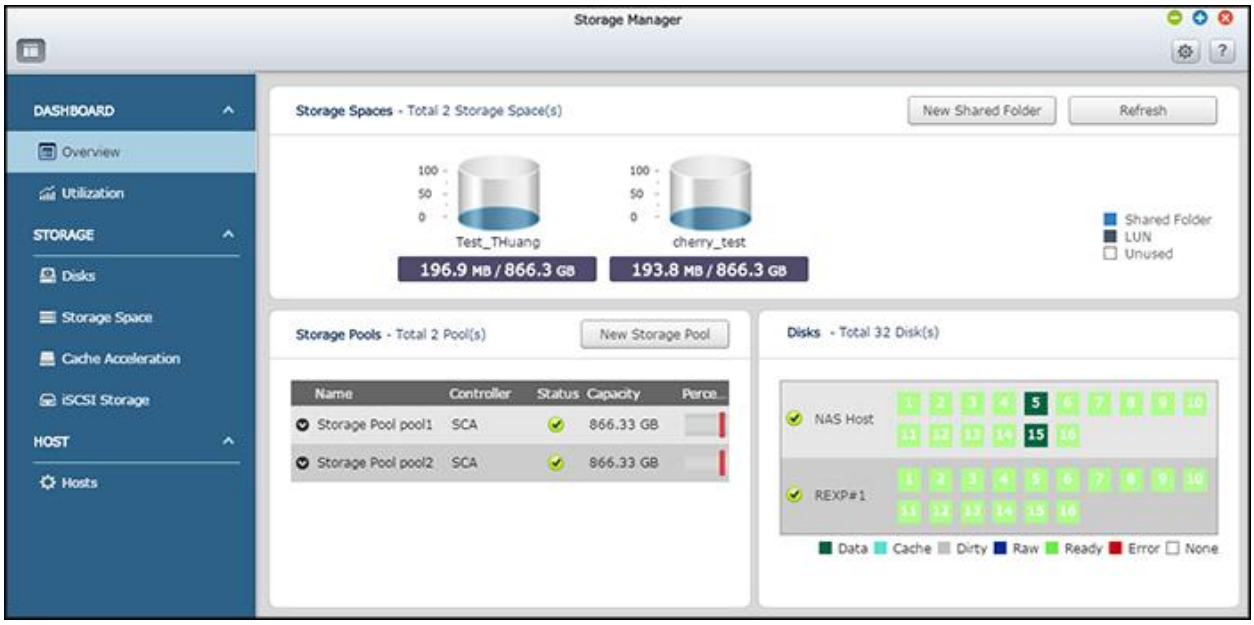
After applying the setting, the NAS will automatically re-check the validity of all passwords set by local NAS users.

Login Screen

Set the login screen style. After you select the style, click "Preview" to preview the chosen template or "Apply" to apply the chosen login screen.

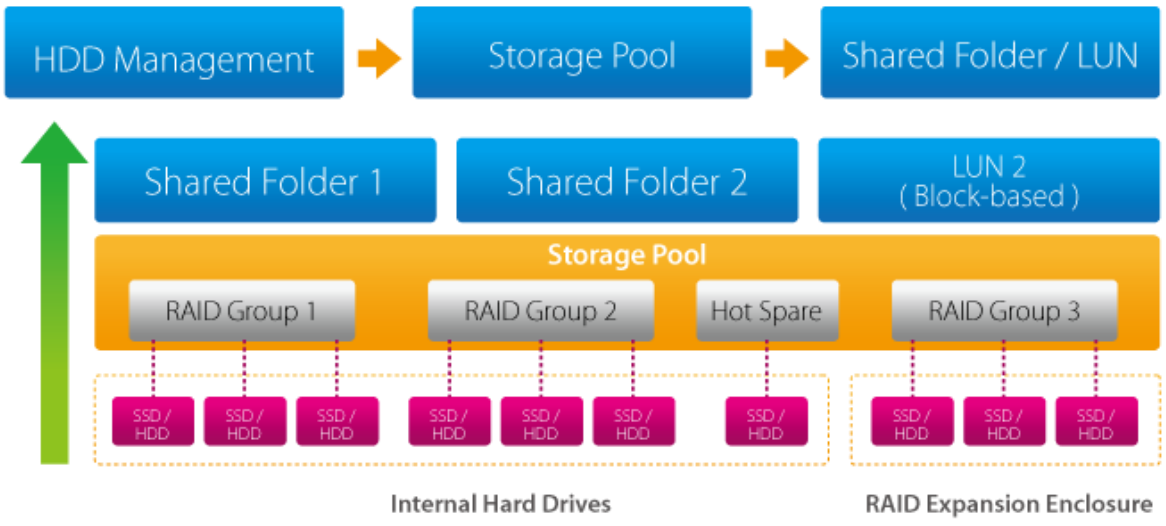
Storage Manager

Based on QNAP's Flexible Volume Architecture, the Storage Manager provides a secure, flexible and comprehensive approach to manage data on your NAS and offers a number of great features such as storage pools, multiple RAID groups, and online capacity expansion. These features can effectively protect your storage system and your valuable data.



QNAP Flexible Architecture

The QNAP Flexible Architecture consists of the following three layers: Disks (HDD Management), Storage Pool and Shared Folders/LUN. Each layer is designed to cover an aspect of the storage system, and all three layers combined can achieve total protection for your storage system.



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

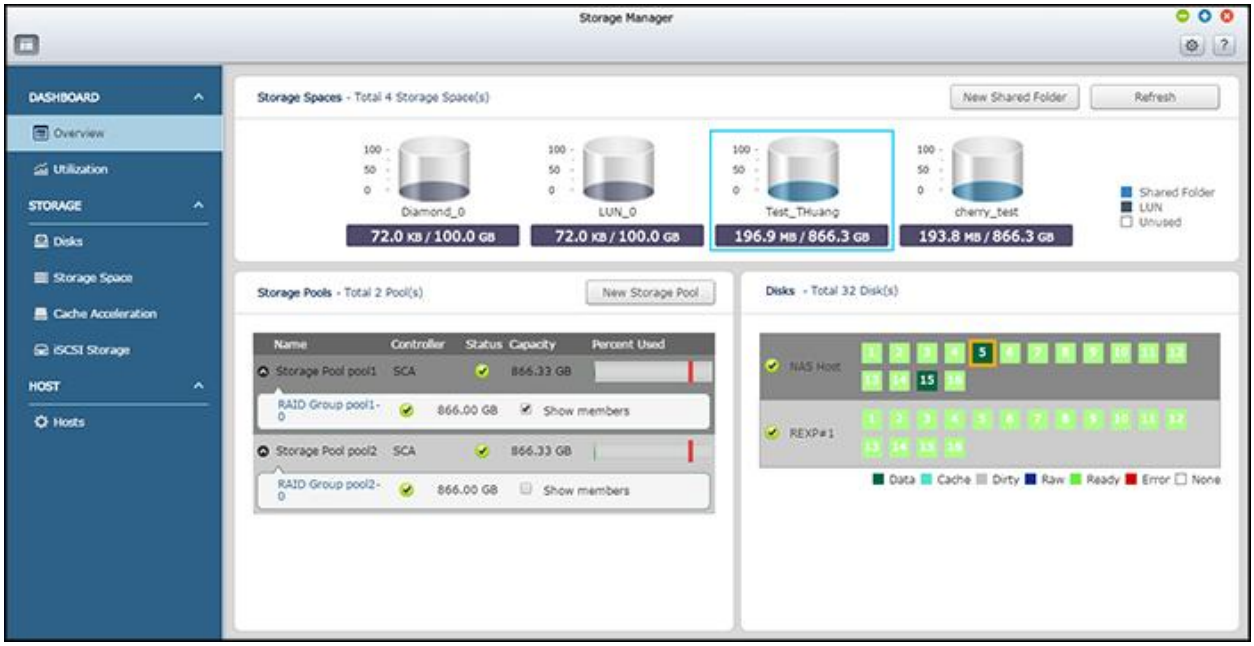
- Dashboard
- Storage
- Host

Note:

- QNAP expansion enclosures are strongly recommended for the best compatibility in expanding the storage capacity of your ES NAS. Refer to the product specification table for more information regarding the maximum number of expansion enclosures supported by each model.

Dashboard

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



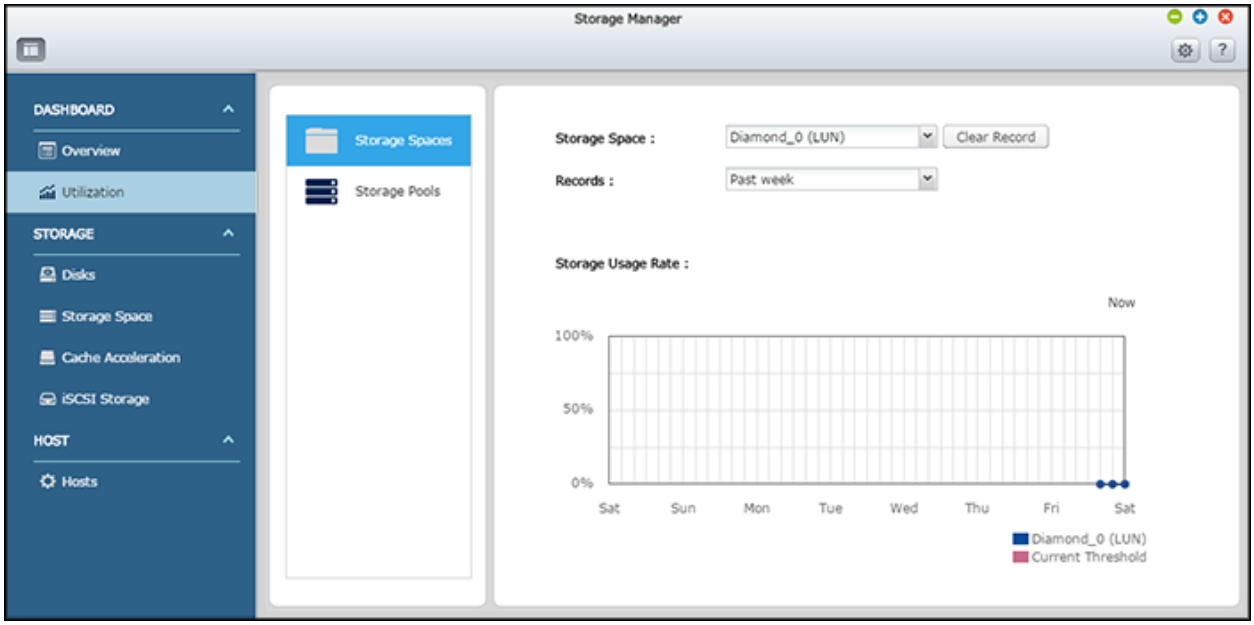
Overview

There are three sections on the page: Storage Spaces, Storage Pools and Disks. They are described below:

- Storage Spaces (Shared Folder/LUN): All available shared folders, their capacity and type (shared folders, LUN and unused) are listed in this section. Check the Shared Folders and iSCSI Storage chapters for more details.
- Storage Pools: This section provides a space usage overview on the storage pool created on the NAS. The name, controller, status, total and used capacity, and RAID group of each storage pool is listed here. Click the down arrow button in front of the name to show its RAID group and "Show members" (in the appeared RAID Group bobble) to check the disks that belong to the RAID group. You can also click "New Storage Pool" in this section to create a storage pool. For details on storage pools, please refer to the Storage Pools chapter.
- Disks: 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.

Utilization

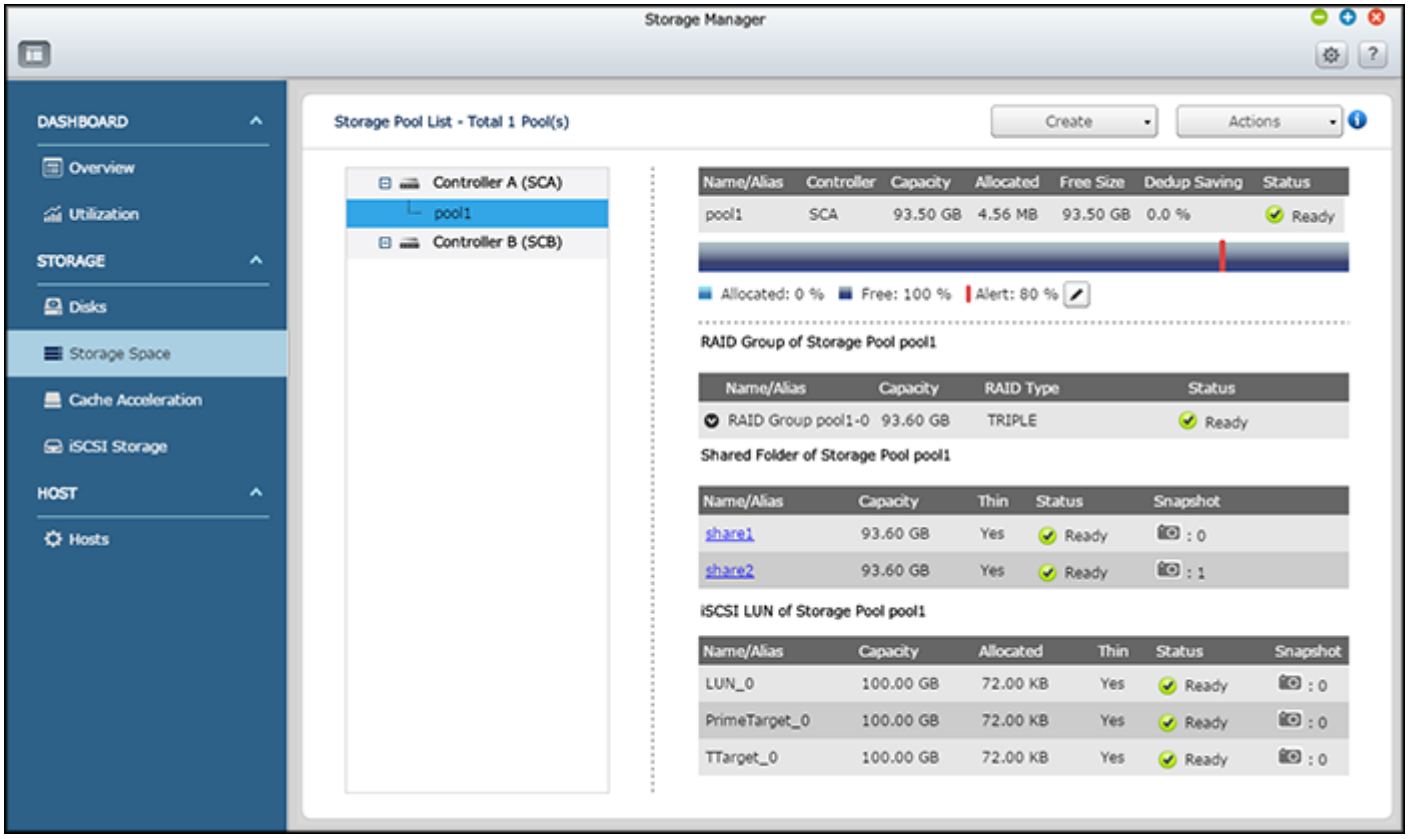
This page is designed for users to monitor storage utilization of their NAS. With storage pool usage information presented on this page, users can manage their storage system more effectively and spot potential issues based on trends over a period of time, from the past hour to the past year.



Select to view the storage usage rate of a particular LUN, shared folder, or storage pool (switch to "Storage Spaces" for a LUN and shared folder; Switch to "Storage Pools" for a storage pool) over a period ranging from the past hour to the past year. Click "Clear Record" to reset the utilization graph.

Storage

Manage storage pools, hard disk drives, shared folders, snapshots, and iSCSI targets and LUNs, encrypt and decrypt file systems, and configure cache acceleration and host white list with Storage Manager.

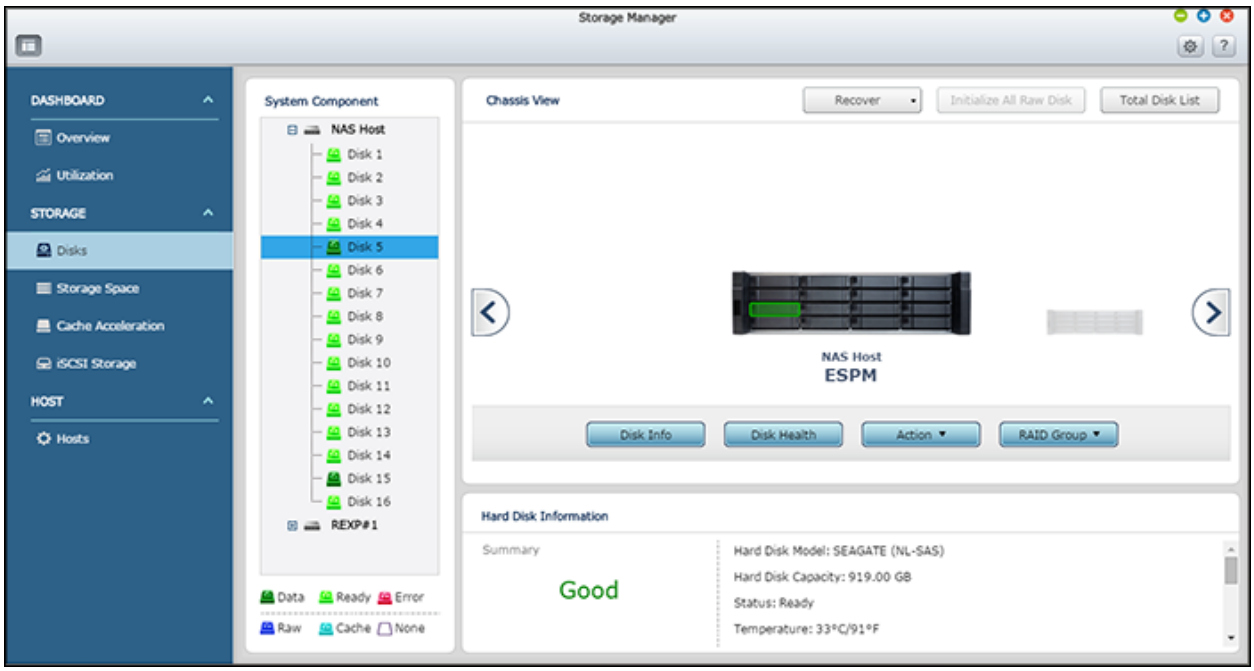


For details on the features, refer to the following links:

- Disks
- Storage Space
- Cache Acceleration
- iSCSI Storage

Disks

This page is designed for users to monitor and manage hard disk drives installed on the NAS and its connected expansion enclosures, and users can quickly isolate and identify hard drives for relevant maintenance tasks.



This chapter covers the following topics:

- Managing NAS Hosts
- Managing Disks
- HDD S.M.A.R.T Information
- Configuring Disk Health Global Settings
- Managing Expansion Enclosures
- Recovering Expansion Enclosures
- Listing all Disks

Managing NAS Hosts

Click a 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 for each controller, system temperature for each controller, power status for each PSU, and system and power fan speed for each power and system fan.
Locate	Click this button and the chassis LEDs of the selected NAS host will blink for easy

(under "Action")	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.

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:

- Data: A disk that contains data.
- Ready: A disk that is ready and healthy.
- Error: A disk detected with errors (could be bad sectors or I/O errors). This disk should be replaced immediately.
- Raw: A disk that has not been initialized.
- Cache: A disk configured as cache.
- Dirty: A disk that was previously in a storage pool, but has been removed from the pool and replaced by a hot spare disk. The occurred due to one of the following reasons:
  - QES detected I/O errors on the disk, and automatically removed it from the pool.
  - A user physically unplugged the disk, a spare disk replaced it in the pool, then the user plugged the disk in again.

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 disk model, model number, serial number, disk 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	Click this button to locate drives using LED lights for easy identification of physical

"Action")	hard drives.
RAID Group	Click this button and select a RAID group and check its details, including capacity, RAID group name, RAID type and disk member.

Disk Health

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.
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 disks" to apply the settings configured on this page only to the currently selected drive or "Apply to All Disks" to all drives (HDD and SSD). Click “Apply to all HDD” to apply the settings to all mechanical hard drives in the NAS, or “Apply to all SDD” to apply the settings to all solid state drives.

Configuring 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):

- Disk S.M.A.R.T polling time (minutes): Specify how often the disks are scanned for S.M.A.R.T errors. The default is every 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.
- Delete the oldest snapshots when a storage pool is full: QES will automatically delete old snapshots when there is no free storage pool space. You can specify snapshots taken on a schedule, snapshots taken manually by a user, or both.
- Enable temperature alarm for hard disk drives: Specify a global temperature alert for all mechanical HDDs in the NAS. Modifying this setting overrides the individual disk settings at "Storage Manager" > "Disks" > [Select a disk] > "Disk Health" > "Settings" > "Enable temperature alarm".
- Enable temperature alarm for solid state drives: Specify a global temperature alert for all solid state drives in the NAS. Modifying this setting overrides the individual disk settings at "Storage Manager" > "Disks" > [Select a disk] > "Disk Health" > "Settings" > "Enable temperature alarm".

Managing Expansion Enclosures

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, 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.
Rename enclosure (under "Action")	Click this button to rename the chosen enclosure.

Recovering Expansion Enclosures

Click "Recover" on the top-right side of the window and click "Reinitialize enclosure ID" to reorder ID for expansion enclosures in a numerical manner.

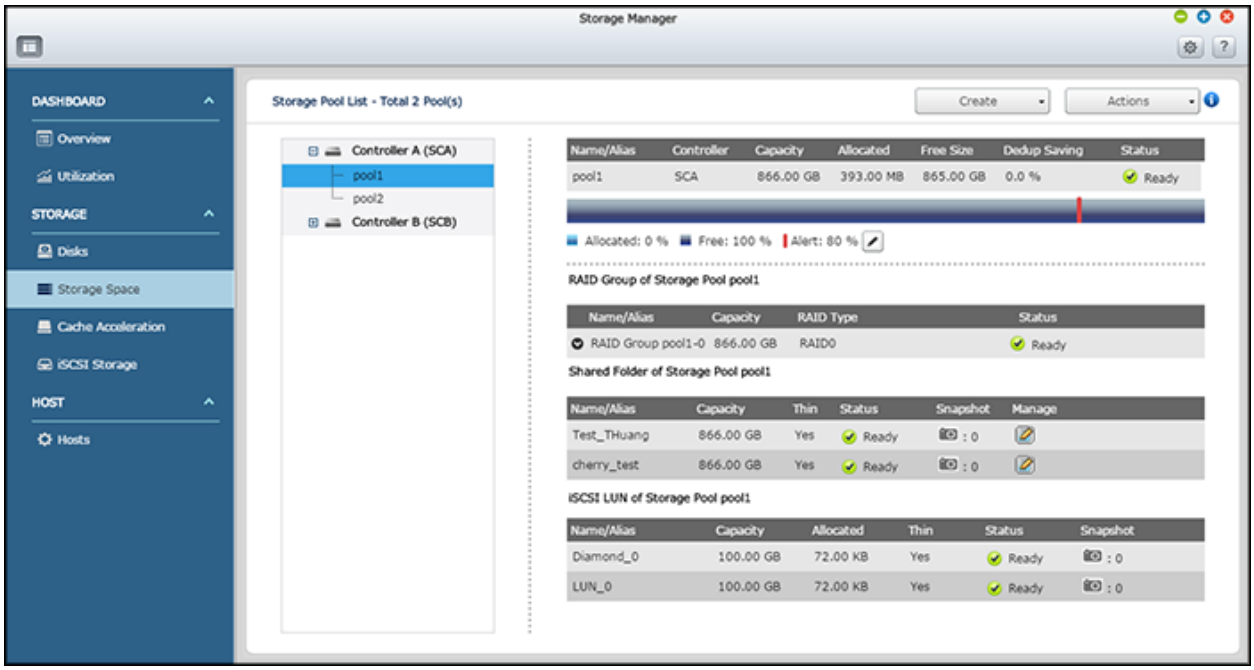
Listing all Disks

Click "Total Disk List" on the top-right side of the window to list all disks. Set the filter from the drop down list to only show hard disks based on the device (enclosure or NAS they belong to), disk, model, type (HDD or SSD), BUS type, capacity, used type (data, ready, error, raw, cache, dirty) and status. Click "Refresh" to refresh the list.

You can also perform a sequential read test using the "Performance test" button, schedule weekly sequential read tests using the "Weekly Test" button and check the test results to gauge the performance of the tested disks.

Storage Space

This page lists available controllers, storage pools, shared folders, iSCSI LUNs and snapshots based on their hierarchical structure. It displays these storage entities' capacity and/or usage to give a complete view of storage allocation. Users can create or manage storage pools/shared folders/RAID groups/iSCSI LUNs, or take/view snapshots of the shared folders/iSCSI LUNs on this page.



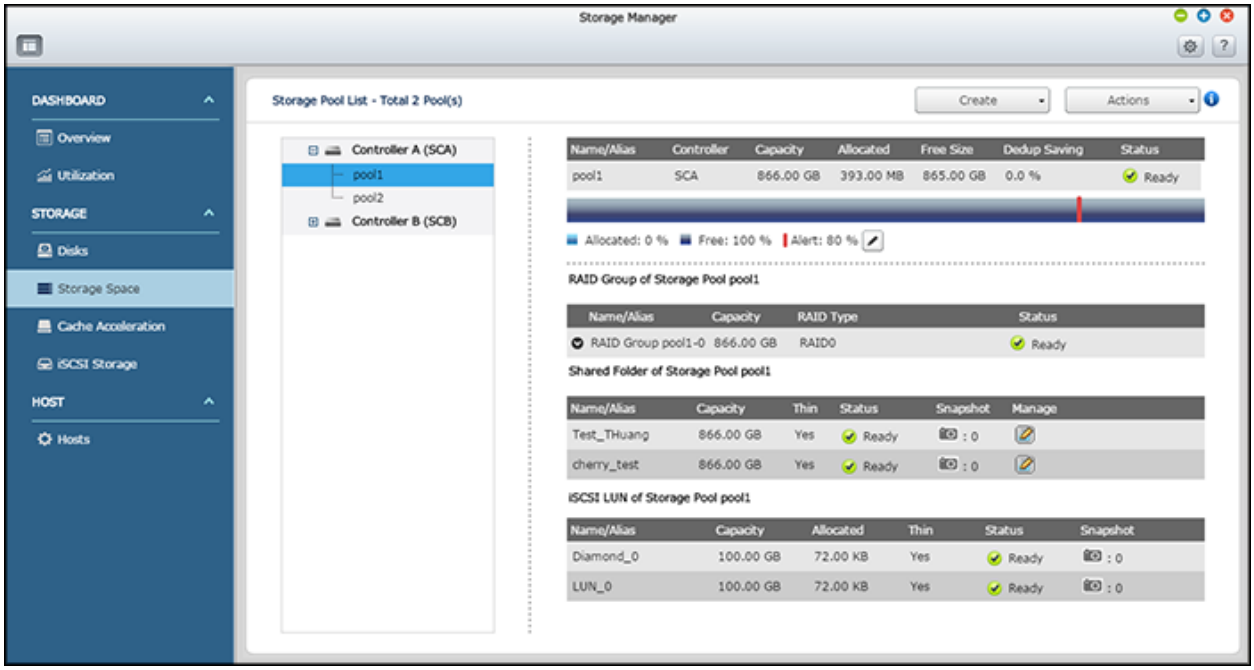
For details on storage pools, RAID groups, and shared folders, refer to the following links:

- Storage Pools
- Shared Folders

Note: You can also create an iSCSI LUN on this page (Click "Create" > "New iSCSI LUN"). For details on creating new iSCSI LUNs, refer to the iSCSI Storage chapter.

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
- Expanding Storage Pools
- Scrubbing Storage Pools
- Offlining and Onlining Storage Pools
- Setting a Threshold

Additionally, RAID group types are covered in this chapter.

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. Specify the pool name, choose the controller the pool belongs to, and select the enclosure unit, hard disk drive(s), RAID type and click "Next".
4. Review the pool creation summary and click "Create".
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.

Note: To configure a spare disk in QES, ensure that there is an initialized free disk with the status

"Ready". This disk can be used as a global hot spare for any storage pool, or for disk ready to be grouped in a pool.

Removing Storage Pools

Follow these steps to remove a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Navigate to the storage pool to be removed.
3. Click "Actions" > "Remove Pool".
4. Click "Apply".
5. The selected storage pool will be removed.

Note: Before you remove a storage pool, be sure to remove all shared folders and LUNs on that storage pool.

Expanding Storage Pools

A storage pool can be expanded by selecting one or more free disks. QES uses these disks to create a new RAID group, and then combines it with other RAID groups in the pool using striping.

The new RAID group must have the same RAID type as all existing RAID groups in the pool. Therefore the number of disks required for expansion is dependent on the existing RAID type of the pool.

Pool RAID Type	Disks required to expand pool
RAID 0	≥ 1
RAID 1	2
RAID 5	≥ 3
RAID 6	≥ 4
RAID-TP	≥ 5
Triple Mirror	Multiple of 3
RAID 10	Multiple of 2
RAID 50	≥ 3 for each additional RAID 5 group
RAID 60	≥ 4 for each additional RAID 6 group

Follow these steps to expand a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Navigate to the storage pool to be expanded.
3. Click "Actions" > "Expand Pool".

4. Select the hard drive(s) to expand the storage pool with and click "Expand".
5. The chosen storage pool will be expanded.

Scrubbing Storage Pools

Scrubbing a storage pools allows you to scan the sectors of RAID groups within that storage pool. QES will automatically attempt to repair failed blocks to maintain the file system's consistency. Please note that during scrubbing, the read/write performance may be affected. Follow these steps to scrub a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Navigate to the storage pool to be scrubbed.
3. Click "Actions" > "Scrub Pool".
4. The chosen storage pool will be scrubbed.
5. (Optional) To stop a running scrubbing task, click "Actions" > "Stop Scrubbing Pool".

Offlining and Onlining Storage Pools

To take a storage pool offline:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a storage pool.
3. Click "Actions" > "Offline Pool".
4. The storage pool will go offline.

To bring an offline storage pool back online:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a storage pool.
3. Click "Actions" > "Online Pool".
4. The storage pool will be brought back online.

Setting an Alert Threshold

QES will generate a warning message in the system logs when the storage pool used size reaches the threshold. To specify the threshold for a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a storage pool.
3. Click the "edit" button (a pen icon) under the storage pool section (right portion of the window).
4. Enter a value for the alert threshold and click "Apply".

Explaining RAID Group Types

Refer to the table below for explanations on RAID types:

Field	Description
RAID 0	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. 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	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. 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. 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.
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. 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.
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. 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 2 failed disks from 2 different pairs are allowed in RAID 10.
RAID 50	RAID 50 is a combination of RAID 5 (distributed parity) and RAID 0 (striping). It is recommended for applications that require high fault tolerance, capacity, and random access performance. RAID 50 requires a minimum of 6 drives and can overcome up to one drive failure in each RAID 5 array. 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.
RAID 60	RAID 60 is a combination of RAID 6 (distributed double parity) and RAID 0 (striping). It offers higher fault tolerance than RAID 50, but uses an extra drive per set for parity. RAID 60 requires a minimum of 8 drives and can overcome up to two drive failures in each RAID 6 array. 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.
Triple Mirror	Triple mirror aims to solve RAID 1 data loss risk if both the primary and mirror drive fails or if there is a non-recoverable read error. Triple mirror writes data simultaneously to three separate HDDs so if two HDDs fail or there are unrecoverable read errors in the same mirror, the system still has access to data with no degradation in performance even as the drives are rebuilt. The advantage is performance; the disadvantage is far less usable capacity.
RAID-TP	RAID TP (disk striping with triple distributed parities) is similar to RAID 5 and 6. It stripes data across drives, but calculates for three parities that are written to three individual disks. RAID-TP uses three independent equations to calculate each individual parity that enables reconstruction of data when three disks and/or blocks fail at the same time. RAID-TP can add an extra level of redundancy to help protect your data. RAID-TP requires a minimum of 4 drives.

RAID Group Capacity

ES NAS use the ZFS RAID scheme RAID-Z. RAID-Z capacity is calculated differently from normal RAID levels. You can use our online calculator to estimate the storage capacity of a RAID group.

1. Go to https://enterprise-nas.qnap.com/en/calculator.
2. Specify the number of disks.
3. Specify the capacity of each disk.
4. Select a RAID type.

Creating RAID 50 and RAID 60 Storage Pools

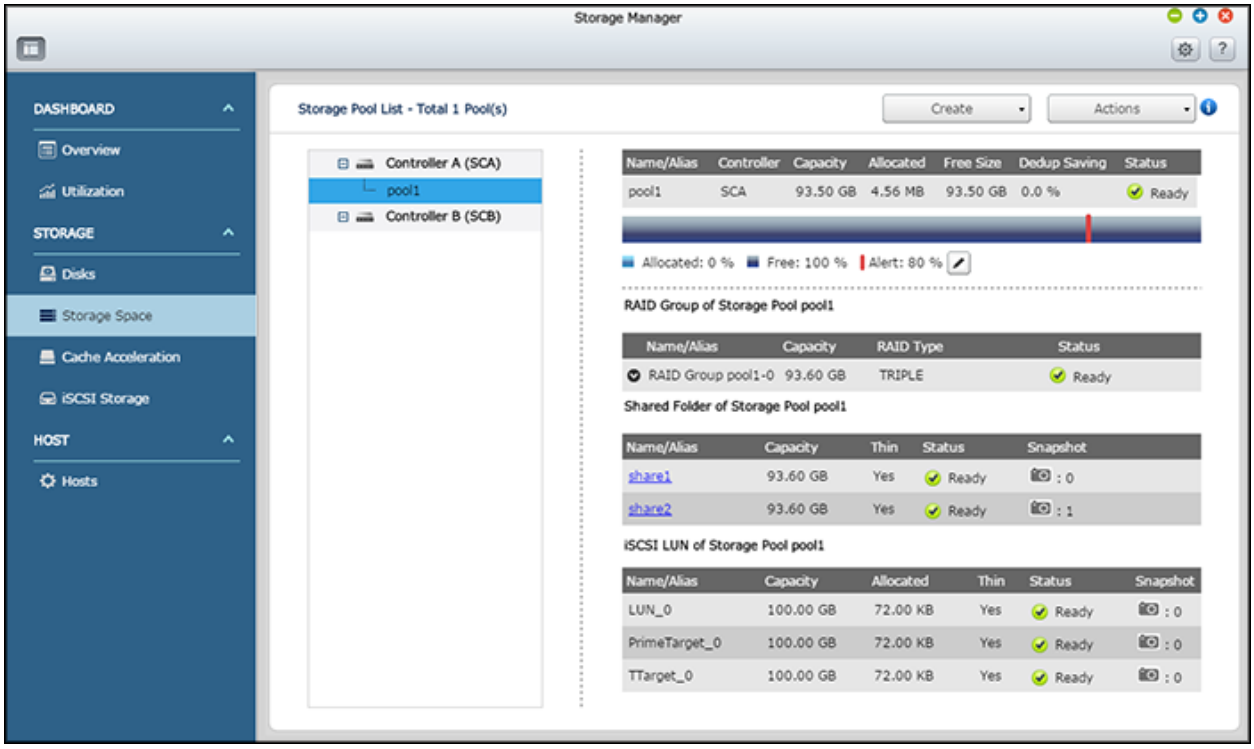
RAID 50 and RAID 60 groups are created at the storage pool level. When multiple RAID groups are added to one pool, QES stripes them using RAID 0. To create a RAID 50 or 60 pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Click "Create" > "New Storage Pool".
3. Create a storage pool of type RAID 5 (for RAID 50) or RAID 6 (for RAID 60).
4. After finishing, navigate to the storage pool and click “Actions” > “Expand Pool”.
5. In the “Expand Pool” wizard, select disks to create another RAID 5 group (for RAID 50), or another RAID 6 group (for RAID 60).
6. Click “Expand”.

The storage pool is expanded, and is using RAID 50 or 60.

Shared Folders

Go to "Storage Manager" > "STORAGE" > "Storage Space" to create, configure, encrypt, and manage shared folders and their snapshots on your NAS.



This chapter covers the following topics:

- Creating Shared Folders
- Deleting Shared Folders and Changing Folder Properties
- Configuring Shared Folder Permissions
  - User and user group permissions
  - NFS host access
  - Microsoft networking host access control
- Encrypting Shared Folders
  - Encrypting and locking a shared folder
  - Encryption verification
  - Unlocking a shared folder
  - Encryption management
- Managing Snapshots
  - Taking a snapshot
  - Managing snapshots with Snapshot Manager
  - Configuring snapshot global settings

Creating Shared Folders

You can create multiple shared folders on one storage pool and specify the access rights of the users and user groups to the shared folders.

To create a shared folder, follow the steps below:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a storage pool.
2. Click "Create" > "New Shared Folder".
3. Enter the basic folder settings for the shared folder.
   - Folder name: Enter the share name. The share name does not support " / \ [ ] : ; | = , + * ? < > ` ' @ ! # % $ ( ) & ^ ~ { } and all double byte characters.
   - Description: Enter an optional description of the shared folder.
   - Storage Pool: Select the storage pool on which to create the folder.
   - Shared Path: Shows all available CIFS/SMB paths to this folder.
   - NFS Path: Shows all available NFS paths to this folder.
4. Configure storage settings and services:
   - Storage settings:
     - Thin provision: Allows the system to over-allocate the storage capacity regardless of the physical storage limit, and the physical disk space is used only when files are written into shared folders.
     - Folder quota: Set the quota of the shared folder. If the quota is not specified, the capacity of the shared folder will be equal to that of the pool.
     - Compression: This option tries to reduce the size of share folder by compressing the data, improving storage space utilization. Enabling this feature consumes CPU resources.
     - Deduplication: This option, once checked, allows the system to reduce the amount of storage needed by eliminating duplicate copies of repeating data. There are three options: "SHA256", "SHA512" and "Skein". Please note that before QES 1.1.3, the default Deduplication option is "SHA256". Data may become inaccessible if you change the option to "SHA512" or "Skein" after updating the firmware.
     - SSD cache: Perform read caching on this shared folder. Data from this folder will be added to the SSD cache.
     - Storage services: Make the shared folder accessible via CIFS/SMB (Windows, Mac), NFS (Linux) or by FTP/FTPS.
5. Configure 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.
6. Advanced settings
   - Hidden Folder: Select to hide the shared folder or not in Microsoft Networking. When a shared folder is hidden, the folder can still be accessed using its full path. For example: \\NAS_IP\share_name.
   - 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.

- Synchronous I/O: Select the ZFS Intent Log I/O mode, to improve data consistency or performance:
  - Always: All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but has a non-negligible impact on performance.
  - Standard: The system uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request.
  - Disabled: All I/O transactions are treated as asynchronous. This option gives the highest performance, but has a higher risk of data loss in the event of a power outage. Ensure that a UPS (uninterrupted power supply) is installed before enabling this option.
- 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".

7. WORM (Write once read many): If enabled, files cannot be modified after they are written to the shared folder. This ensures that data cannot be tampered with. There are two main WORM options.
   - Enterprise: Users are able to delete the shared folder.
   - Compliance: Users are unable to delete the shared folder. A user must remove the storage pool to delete the WORM shared folder.

> **Note:** Enabling "retention" limits how long WORM is applied to files. If enabled, files cannot be modified within the specified time period after being written to the shared folder.

8. Folder Encryption: Select to enable folder encryption (with 256-bit AES encryption) using a password or a key. See Encrypting Shared Folders for more information.
9. Click "create" to complete the setup.

> **Tip:**
> - You can also create a shared folder in File Station. Check the File Station chapter for details.
> - The asynchronous file I/O is generally considered more efficient, but if power outage occurs, and the file writing process using the asynchronous file I/O is interrupted, data loss may happen.

Deleting Shared Folders and Changing Folder Properties

To delete a shared folder, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space", find and click the shared folder.
2. Click "Actions" > "Remove" > "Apply".

To edit the properties of a shared folder, follow these steps:

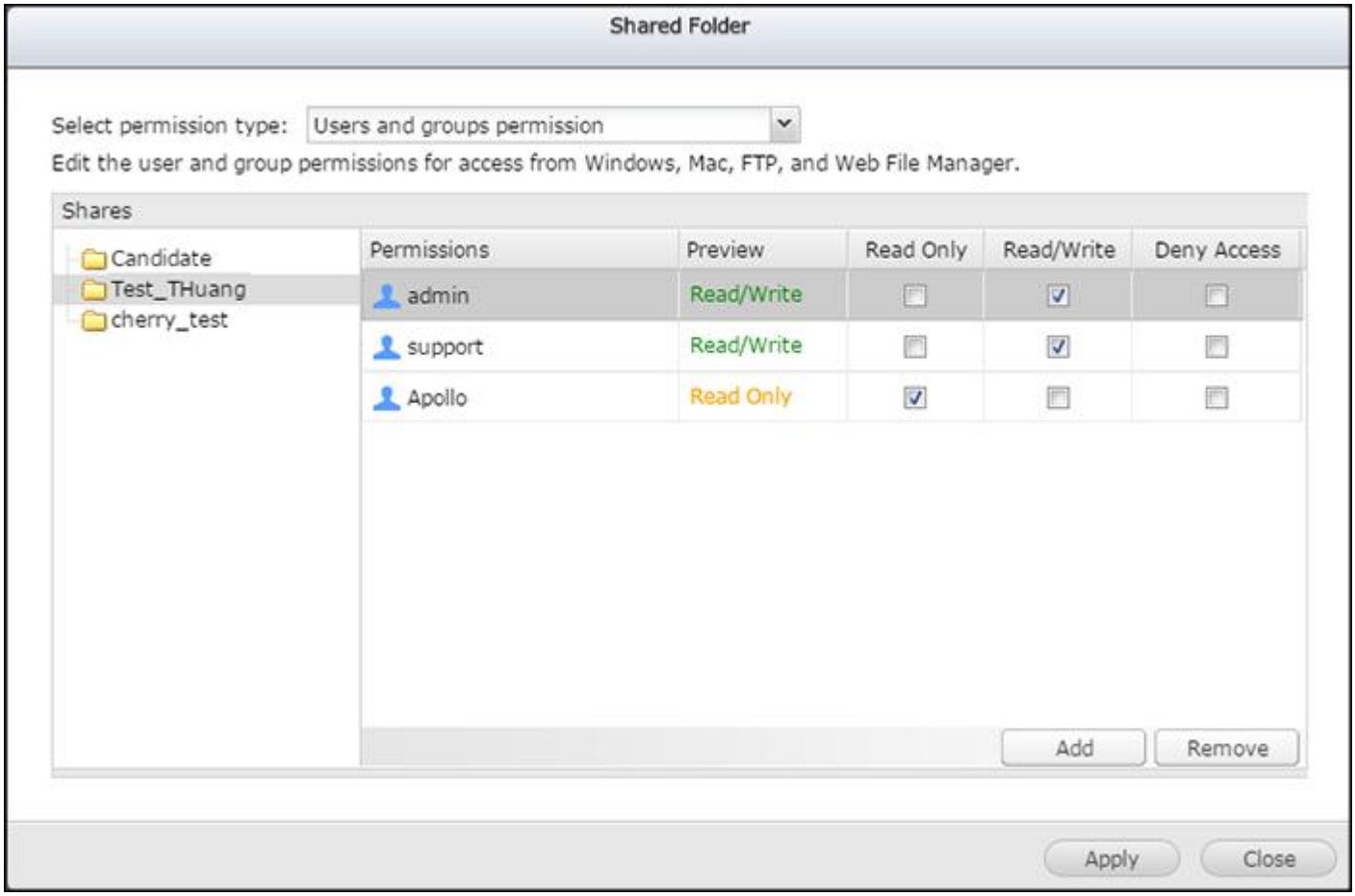
1. Go to "Storage Manager" > "STORAGE" > "Storage Space", find and click the shared folder.
2. Click "Actions" > "Edit Properties".

The properties that can be changed include the folder name, description, storage settings (including Thin Provision, Folder Quota, Compression, Deduplication and SSD Cache) and services (CIFS/SMB, NFS, FTP/FTPS), and advanced settings (Hidden Folder, Oplocks, Synchronous I/O, and Recycle BIN. Refer to the Creating Shared Folders section above for details (in Step 4 and 6).

Note: If deduplication is disabled after being enabled, then newly written data will not be deduped. However, all existing deduped data will remain deduped.

Configuring Shared Folder Permissions

There are three types of permissions users can configure for shared folders: 1) user and group permissions; 2) NFS host access; and 3) Microsoft Networking host access. To configure these permission types, locate and click the shared folder in "Storage Manager" > "STORAGE" > "Storage Space" and select "Permissions".



User and group permissions

Select "Users and groups permission" from the "Select permission type" drop-down list. The folder name will be shown on the left and the users with configured access rights are shown in the right panel. Click "Add" to select more users and user groups on the NAS or from the domain and specify their access rights to the folder. Click "Add" to confirm addition. Or, you can click "Remove" to remove any configured permissions. You can select multiple items by holding the Ctrl key and left clicking the mouse. Click "Apply" to save the settings.

Note:

- If you have specified "deny access" for a user on the root folder, the user will not be allowed to access the folder and subfolders even if you select read/write access to the subfolders.
- If you 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 permissions on the root folder and read/write permissions on the subfolders, you must set read/write permissions on the root folder.

NFS host access

This permission type specifies if hosts connecting to the NAS by NFS are allowed to access the shared folder.

- Support NFSv4 ACL Inheritance: Unselect this option to disable NFSv4 ACL Inheritance and enable umask settings.
- Enable Map_Root and Map_All: When a user connects to the NFS share, they connect with the permissions associated with their user account. This can cause security risks, especially if the user has root privileges. Map_Root and Map_All enabled you to restrict a connected users permissions. Only one option can be selected. To restrict the root user's permissions, set the Map_Root option. To restrict the permissions of all users, set the Map_All option.
    - Map_Root: If the root user connects to the NFS share, they will be limited to the specified user and group permissions.
    - Map_All: All users connecting to the NFS share will be limited to the specified user and group permissions.
- Access right: The default is “Deny access”, which means no hosts can access the shared folder using NFS. To grant a host access:
    1. Select “No Limit” or “Read only” under “Access right”.
        - No limit: 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.
    2. (Optional) Select “All hosts can access the shared folder” to apply the selected access rights to all NFS hosts.
    3. Select a host in the hosts table.

a. IF the host does not exist in the table, click “Create Host” and specify its IP address or network name.

4. Click “Apply”.

Microsoft networking host access control

Shared folders can be accessed by Windows and Linux hosts via Samba by default. You can still specify the authorized hosts for certain shared folders by following these steps:

1. Select "Microsoft Networking host access" from the drop-down menu on top of the page.
2. Uncheck "All hosts can access the shared folder".
3. Specify the allowed host names, or click "Create Host" if your desired hosts are not on the list.
4. click "Apply".

Encrypting Shared Folders

Shared folders on the NAS can be encrypted with 256-bit AES encryption to protect data. The encrypted shared folders can only be accessed with the authorized password. The encryption feature protects the confidential data of the folder from unauthorized access even if the hard drives or the entire NAS are stolen.

Note: The encryption key cannot include dollar signs ($) or equal signs (=).

Encrypting and locking a shared folder

To encrypt and lock a shared folder:

1. When first creating a shared folder, tick "Encryption" under "Folder Encryption", enter a password and choose to save an encryption key.
2. Click "Actions" > "Encryption" in the "Shared Folder Manager" dialog, switch to "Lock it" and click "OK".

Encryption verification

After a folder is locked, that folder will not appear 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, click "Actions" > "Encryption" in the "Shared Folder Manager" dialog and enter the password or upload the encryption key file. The encryption key can be downloaded by clicking Actions" > "Encryption" > "Download" when the shared folder is unlocked.

Encryption management

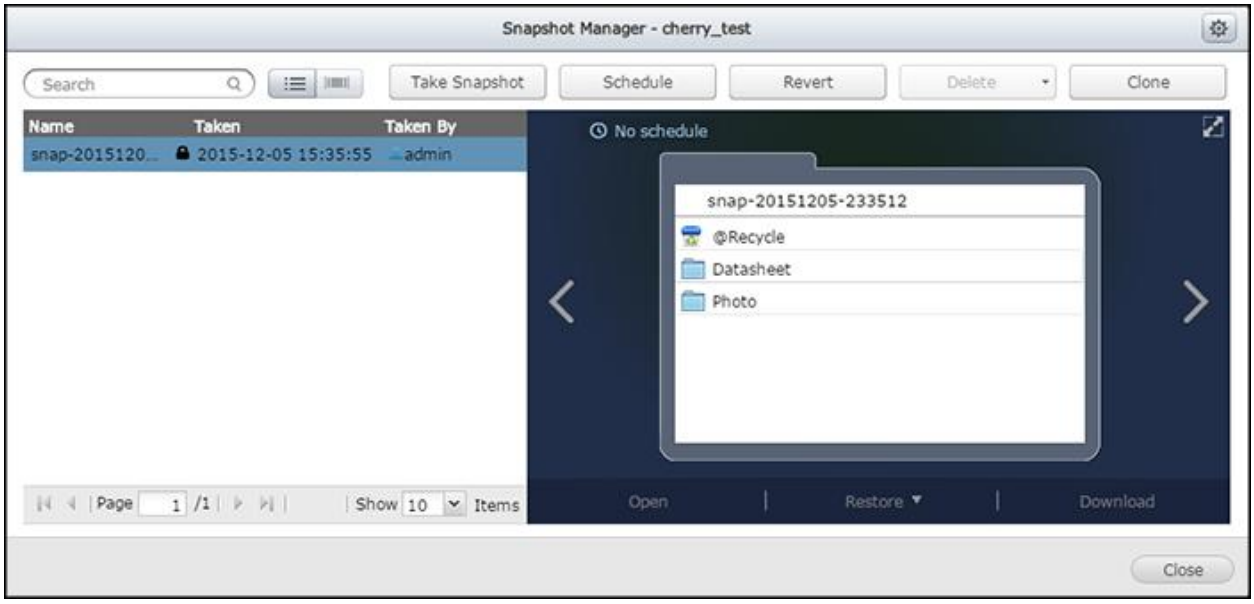
After encryption is enabled for a shared folder, click "Actions" > "Encryption" in the "Shared Folder Manager" dialog to manage the encryption key for that shared folder. For encryption key management, you can change the password and save, download, and unsave the encryption key.

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 path.

Managing Snapshots

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



Note: Snapshot replication (or shared folder/LUN replication between remote servers) is covered in Backup Station. For details, please refer to the SnapSync chapter in Backup Station.

Taking a snapshot

To create a snapshot, follow these steps:

1. Click the camera icon of a shared folder or LUN in "Storage Manager" > "STORAGE" > "Storage Space" to launch the Snapshot Manager and click "Take Snapshot". For a shared folder, you can also click "Snapshot" > "Take a Snapshot" in the "Shared Folder Manager" dialog.
2. Specify the snapshot name and duration to retain the snapshot.
3. 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 the Snapshot Manager, click the camera icon of a shared folder or LUN in "Storage Manager" > "STORAGE" > "Storage Space". For a shared folder, you can also click "Snapshot" > "Snapshot Manager" in the "Shared Folder Manager" dialog.

In Snapshot Manager, you can perform the following actions:

- Restore files: Select a snapshot of a shared folder, and then select the folders or files 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. Note: It is not possible to restore files from a snapshot of an iSCSI LUN.
- Revert a snapshot: Select a snapshot and click "Revert", and the entire snapshot will be restored to its original path. Be cautious that the shared folder reverted to the selected snapshot will be in the previous state when the snapshot was taken. Note: iSCSI LUNs must be unmapped before performing the revert.
- Delete: Select a snapshot and click "Delete" to delete that snapshot, or click "Delete all" to delete all snapshots for the shared folder or LUN.
- Clone a snapshot: This action allows you to clone a snapshot into a new shared folder or LUN. To clone a snapshot, first select a snapshot, click "Clone", enter alias of the destination shared folder. 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 automatically take the snapshot according to the specified schedule.

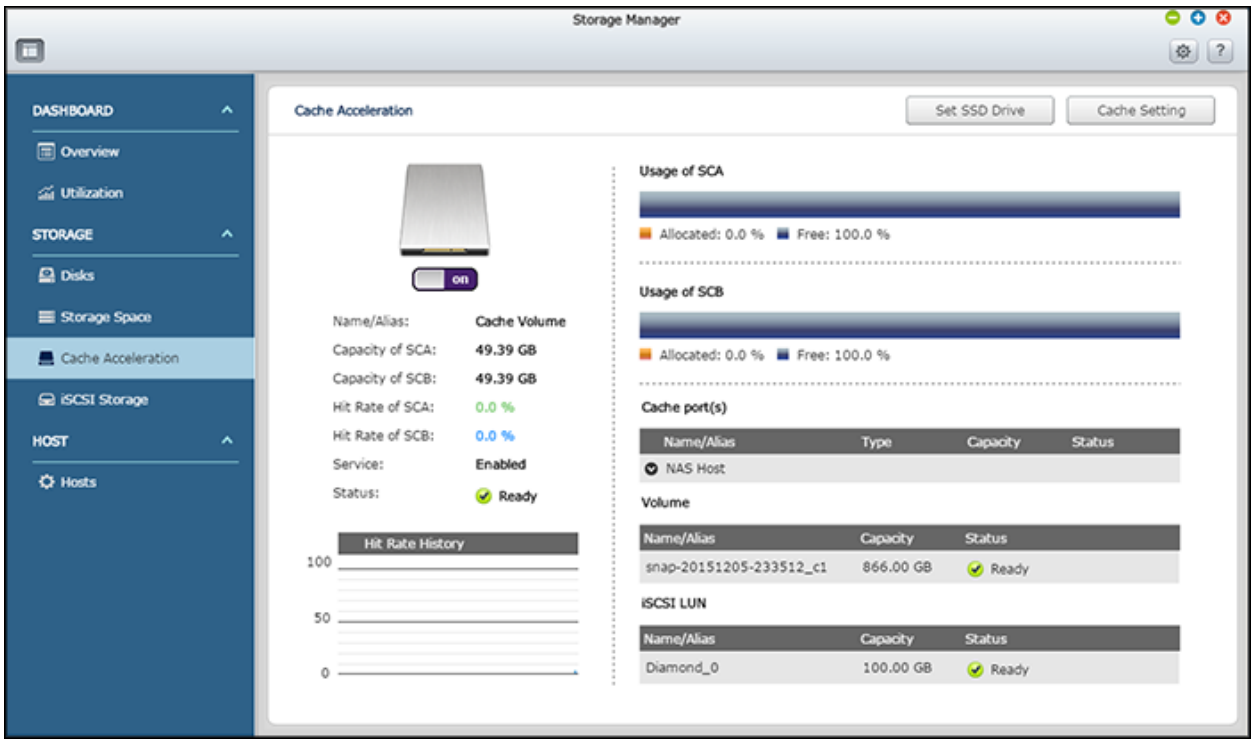
Configuring snapshot global settings

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 as a directory of a shared folder and set the snapshot to be read-only in File Station.

Cache Acceleration

Based on SSD technology, the Cache Acceleration feature is designed to boost access performance of the NAS. On this page, users can choose to create, remove or expand an SSD volume, configure the SSD cache, and monitor SSD cache performance.



This chapter covers the following topics:

- Creating, Removing and Expanding SSD Volumes
- Configuring Volumes for SSD Cache

Note: From QES 1.1.3 onwards, it is possible to use a PCIE NVME SSD for the SSD cache. For details on drives compatible with your NAS, see www.qnap.com/compatibility.

Creating, Removing and Expanding SSD Volumes

Follow the steps below to create, remove or expand a SSD volume:

1. Go to “Storage Manager” > STORAGE” > “Cache Acceleration”.
2. Click "Set SSD".
3. Select the available SSD drive(s):
   - To create a SSD volume, select the desired SSDs and choose to enable RAM write cache protection (see the note box below for more information).
   - To remove a SSD volume, deselect all the SSD drive(s).
   - To expand a SSD volume, select the SSD drive(s) in addition to the ones that have already been chosen.
4. Click "OK".

Note:

- "Enable RAM write cache protection" is only available on TES NAS.
- After enabling "Enable RAM write cache protection", data in the RAM write cache will be backed up to the SSD for data protection. Two or more SSDs are required to enable this option.
- If "Write cache protection" is enabled, the "Write Log" option on the "Cache Acceleration" page will show as "Enabled".
- The system will automatically disable this feature if an SSD fails.

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 or iSCSI LUN to enable/disable the SSD cache, choose whether to enable "Bypass Prefetch Data" 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.

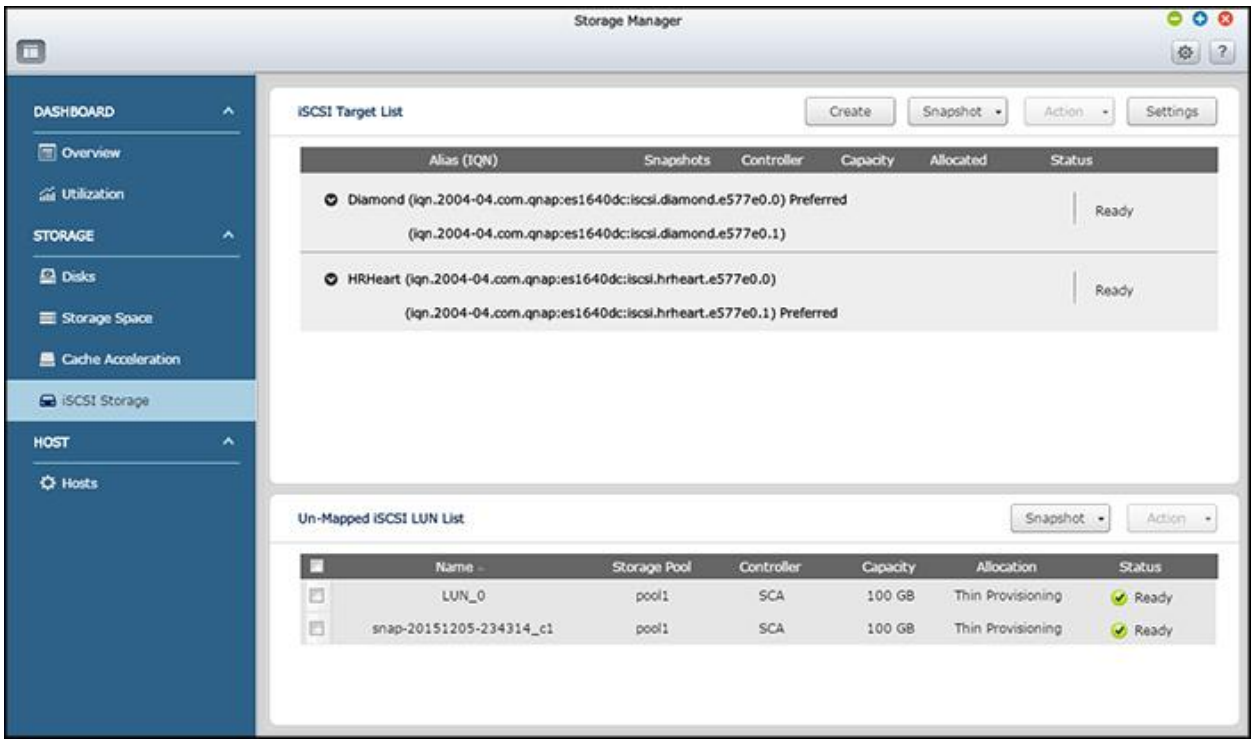
Note:

- 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 an SSD cache. Please make sure that the SSD cache is supported by your applications.
- If the SSD cache service is disabled, QES will stop added new files to the cache volume. However, all existing cached files will remain in the SSD cache. To clear the cache, remove the SSD(s) from the cache volume.

iSCSI Storage

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

Users can enable or disable the iSCSI service, change the port of the iSCSI portal, enable/disable the iSNS service, and list and manage all iSCSI targets and LUNs on this page. The NAS supports multiple iSCSI targets and multiple LUNs per target. iSCSI LUNs can be mapped or unmapped to a specific target.



In this chapter, these topics are covered:

- iSCSI Configuration
  - iSCSI Quick Configuration Wizard
  - Creating iSCSI targets
  - Creating iSCSI LUNs
  - Switching iSCSI LUNs between targets
  - Expanding iSCSI LUN capacity
  - Enabling and disabling iSCSI and iSNS services
- Optimizing iSCSI Performance
- Snapshot
  - Taking a snapshot
  - Managing snapshots
  - Snapshot Agent

iSCSI Configuration

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

1. Install an iSCSI initiator on a Windows, Mac, or Linux server.
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. The ES NAS uses block-based LUNs that support the following features: VAAI Full Copy, VAAI Block Zeroing, VAAI Hardware Assisted Locking, Thin Provisioning, Space Reclamation (with VAAI or from Windows 2012 or 8), Microsoft ODX, LUN Snapshot, and LUN SnapSync.

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.
- Instant Allocation: Allocate the disk space to the LUN instantly. This option guarantees the disk space assigned to the LUN.

A maximum of 255 iSCSI targets and 1024 LUNs can be created. 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.

Warning: It is NOT recommended to connect to the same iSCSI target with two (or more) different clients (iSCSI initiators) at the same time, unless the clients are in the same cluster group. Otherwise, it may lead to data loss or disk damage.

iSCSI Quick Configuration Wizard

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

1. Go to "Storage Manager" > "iSCSI Storage" > "Create" to launch the Quick Configuration Wizard.
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. 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."

5. 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:
   - Use CHAP authentication:
     - Username
       - Valid characters: 0-9, a-z, A-Z
       - Length: 1 to 128 characters.
     - Password
       - Valid characters: 0-9, a-z, A-Z
       - Length: 12 to 16 characters.
   - Mutual CHAP:
     - Username
       - Valid characters: 0-9, a-z, A-Z, : (colon), . (dot), - (dash)
       - Length: 1 to 128 characters.
     - Password
       - Valid characters: 0-9, a-z, A-Z, : (colon), . (dot), - (dash)
       - Length: 12 to 16 characters.
6. Select the interface the target uses for data transfer. Then click "Next".
7. Specify the access rights for existing hosts to access the target or add a new host. Note that at least one host on the list must have the "All Access" access right (You can click the field under "Access" to edit the access right for that host.) Click "Next".
8. Specify the LUN properties, including the followings and then click "Next":
   - Name of the LUN,
   - LUN allocation method (Thin Provisioning or Instant Allocation),
   - LUN location (storage pool on the NAS),
   - Capacity,
   - Alert threshold,
   - Performance profile (generic, hyperv, vmware, database, or custom)
   - Whether to enable synchronous I/O: Select "Always" to always use synchronous file I/O or "Standard" for the system to deploy the file I/O approach (synchronous file I/O or asynchronous file I/O) based on applications. Use the default option if you are not sure which one to choose.
   - SSD cache,
   - Deduplication: There are three options: "SHA256", "SHA512" and "Skein". Please note that before QES 1.1.3, the default Deduplication option is "SHA256". Data may become inaccessible if you change the option to "SHA512" or "Skein" after updating the firmware.
   - Compression, and
   - Encryption for the LUN.

9. Confirm the settings and click "Next".
10. Click "Finish" and the target and LUN will both show up on the list.

Tip: The performance profile in Step 8 relates to how the LUN will be used. There are five options: generic, Hyper-V, VMware, database, or customized. Each option will set a different block size for the created LUN and its performance will differ.
For the "custom" option, you can choose the LUN block size that best suits your application from the following: 8k, 16k, 32k, 64k, 128k.
If you are unsure about which one to choose, select "generic".

Creating iSCSI targets

Follow the steps below to create an iSCSI target:

1. Click "Create".
2. Select "iSCSI Target only" and click "Next".
3. Enter the target name and alias. Select a controller and choose to click "CRC/Checksum" to select "Data Digest" and/or "Header Digest". Then Click "Next".
4. Choose to enable CHAP authentication and 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. Click "Next".
5. Select the interface the target uses for data transfer. Then click "Next".
6. Specify the access rights for existing hosts to access the target or add a new host. Note that at least one host on the list that must have the "All Access" access right (You can click the field under "Access" to edit the access right for that host.) Click "Next".
7. Confirm the settings and click "Next".
8. Click "Finish".
9. 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. Specify the LUN properties, including the followings, and then click "Next":
   - Name of the LUN,
   - LUN allocation method (Thin Provisioning or Instant Allocation),
   - LUN location (storage pool on the NAS),
   - Capacity,

- Alert threshold,
- Performance profile (generic, hyperv, vmware, database, or customized).
  For the “customized” option, you can choose the LUN block size that best suits your application from the following: 8k, 16k, 32k, 64k, 128k.
- Whether to enable synchronous I/O: Select "Always" to always use synchronous file I/O or "Standard" for the system to deploy the file I/O approach (synchronous file I/O or asynchronous file I/O) based on applications. Use the default option if you are not sure which one to choose.
- SSD cache,
- Deduplication: There are three options: "SHA256", "SHA512" and "Skein". Please note that before QES 1.1.3, the default Deduplication option is "SHA256". Data may become inaccessible if you change the option to "SHA512" or "Skein" after updating the firmware.
- Compression, and
- Encryption for the LUN.

4. Choose to map the LUN to a target (if you check "Do not map it to a target for now", the LUN will be created as an un-mapped iSCSI LUN and listed under the un-mapped iSCSI LUN list) and click "Next".
5. Confirm the settings and click "Next".
6. Click "Finish".

The description of each iSCSI target and LUN status is explained below. Select an iSCSI target and the LUNs mapped to it will be shown.

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.
	Offline	The iSCSI target has been deactivated and cannot be connected by the initiator.
LUN	Enabled	The LUN is active for connections 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 for: target alias, CHAP information, checksum, settings, hosts, portals. Modify the LUN settings for: LUN allocation, name, disk volume directory, etc.
Delete	Delete an iSCSI target. All the connections will be removed.
Disable	Disable an LUN. All the connections will be removed.
Enable	Enable an 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 IP and IQN information 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 server (Windows PC, Mac, or FreeBSD) can connect to the iSCSI targets and LUNs, and these volumes can be used as the virtual drives on the computer.

QNAP have produced Application Notes to help users set up iSCSI in different environments and use cases. To see them, go to www.qnap.com/download, enter your NAS model then click “Application Notes”.

Expanding iSCSI LUN capacity

The NAS supports capacity expansion for iSCSI LUNs:

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.

Enabling and disabling iSCSI and iSNS services

To enable/disable the iSCSI service, change the port of the iSCSI portal, or enable/disable the iSNS service, click "Settings".

Optimizing iSCSI Performance

For details on optimization, see the iSCSI specific application notes at www.qnap.com/download.

Snapshot

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:

- Snapshot replication (or LUN replication between remote servers) is covered in Backup Station. For details, please refer to the SnapSync section in Backup Station.
- Application consistent snapshots for iSCSI LUN are only available when the Snapshot Agent is used and for VMware and VSS-aware applications running on a Windows server. For details, see the related application notes at www.qnap.com/download.

Taking a snapshot

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".

Managing snapshots

You can revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files for LUNs or shared folders. For more information on these functions, see Managing Snapshots with Snapshot Manager for shared folders 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. For details on Snapshot Agent, see the QNAP Snapshot Agent release note:

https://files.qnap.com/news/pressresource/datasheet/Create_Microsoft_Hyper-V_Backups_Using_QNAP_Snapshot_Agent_and_VSS_Hardware_Provider(English).pdf

Connecting to iSCSI Targets using Microsoft iSCSI Initiator on Windows

As ES NAS is a dual controller NAS that offers failover protection, we strongly recommend multi-path setup and MPIO installation for iSCSI Target connections.

For detailed instructions, see the iSCSI Microsoft Windows Application Note.
https://files.qnap.com/news/pressresource/datasheet/Configuring_Microsoft_iSCSI_Storage_with_QNAP_Enterprise-Class_ES_NAS(English).pdf

For the latest version, or for other languages:

1. Go to www.qnap.com/download.
2. Specify your ES or TES NAS model.
3. Click "Application Notes".
4. Download the note **Configuring Microsoft iSCSI Storage with QNAP Enterprise-Class ES NAS.**

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 LUN (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. After initialization, you can use the iSCSI LUN as an external drive on your Mac.

Connecting to iSCSI Targets by Open-iSCSI Initiator on Linux

This section shows you how to use the Linux Open-iSCSI Initiator 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.

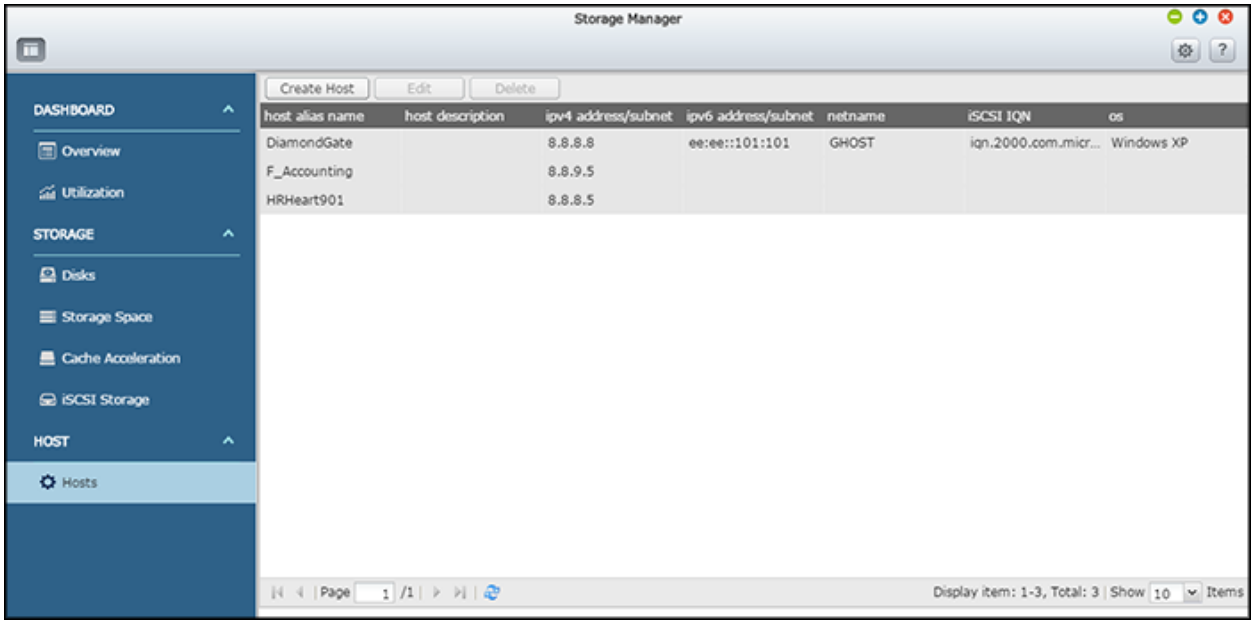
For detailed instructions, see the iSCSI Linux Application Note:
https://files.qnap.com/news/pressresource/datasheet/Configuring-Linux-iSCSI-Storage-with-QNAP-ES-(Enterprise-Storage)-NAS.pdf

For the latest version or for other languages:

1. Go to www.qnap.com/download.
2. Specify your ES or TES NAS model.
3. Click "Application Notes".
4. Download application note: **Configuring Linux iSCSI Storage with QNAP ES (Enterprise Storage) NAS**.

Hosts

Trusted hosts are listed here and you can add, edit, or remove a host on this page. This list will appear when you configure permissions for shared folders and iSCSI LUNs.



Creating, Editing and Deleting Hosts

To create a host, click "Create Host" and specify the host alias name, host description, IPv4 address or subnet, IPv6 address or subnet, network name, iSCSI IQN, and operating system fields for the host. Then click "Apply". For the IPv4, IPv6 address, network name, and iSCSI IQN fields, use "+" or "-" to add or remove an entry.

To edit a host, first select a host in the list and click "Edit". Then add a new entry, or change or remove the existing entry. Then click "Apply".

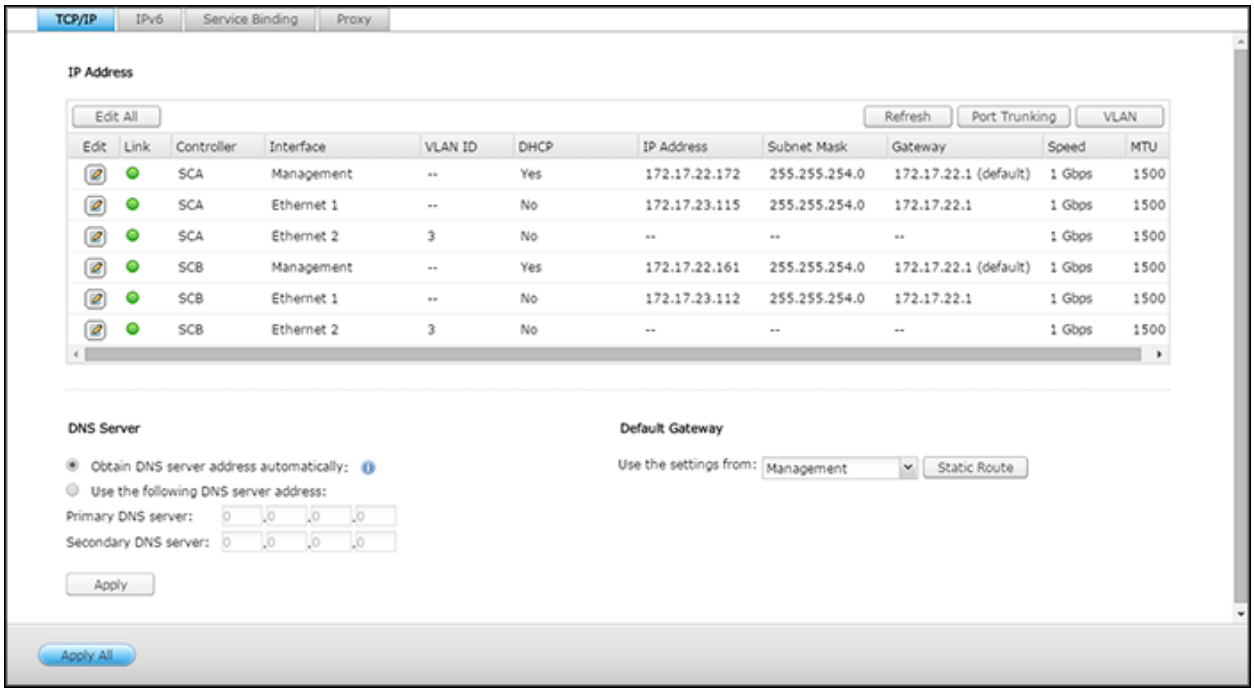
To remove a host, first select a host and click "Delete".

Tip: How do I find the initiator IQN?

- Start the Microsoft iSCSI initiator and click "General". You can then find the IQN of the initiator.
- For VMware ESXi, log in to the vSphere Client, and select an ESXi Host. Go to the “Configuration” tab and click “Storage Adapters” in the “Hardware panel”. (A list of available storage adapters is displayed). Under “iSCSI Software Adapter”, right-click on a vmhba and open “Properties” to view the initiator IQN.

Network

Go to "Control Panel" > "System Settings" > "Network" to configure the NAS network settings.



In this chapter, the following topics are covered:

- TCP/IP
  - IP Address
  - DNS Server
  - Default Gateway
  - Port Trunking
  - VLAN
- IPv6
- Service Binding
- Proxy

TCP/IP

IP Address

Configure the TCP/IP settings, DNS Server and default Gateway of the NAS on this page. You can check and configure IP, port trunking, VLAN, DNS server and gateway settings for all available interfaces, and check link status.

Click the "Edit" button next to an interface to edit its network parameters. The NAS (ES1640dc and ES1640dc v2) by default has one management interface and two Ethernet interfaces on each controller. The management interface is designed for users to access and manage the NAS, but is also used for

network services such as AD, NTP and SNMP. The Ethernet interfaces are dedicated to data transfer, for iSCSI and shared folders.

Users can connect both Ethernet interfaces to two different switches and configure the TCP/IP settings. The NAS will acquire two IP addresses which allow access from two different subnets. This is known as multi-IP settings. When using Qfinder Pro to detect the NAS IP, the IP of Ethernet 1 will be shown in LAN 1 only and the IP of Ethernet 2 will be shown in LAN 2 only. To use port trunking for a dual LAN connection, see section (iv).

Note: You can click "Edit All" to change the IP addresses of all the interfaces and apply all changes at once, instead of one interface at a time.

Network Parameters

After clicking "Edit" next to an interface, you can configure the following:

- Network Speed: Select the network transfer rate according to the network environment of the NAS. Select "Auto-negotiation" and the NAS will automatically adjust the transfer rate.
- 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 for network connections, enter the IP address, subnet mask, and default gateway.

  Note: In QES 1.1.3 and later, you can specify a default gateway for an interface that is part of a VLAN.

- 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. Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can transmit. The NAS uses standard Ethernet frames (1500 bytes) by default. If 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:

- When you access the NAS using a browser, please ensure that you use the IP address of the management interface.
- Jumbo Frames is valid in Gigabit (or faster) networks. Every connected network appliance must enable Jumbo Frames and use the same MTU value. (1Gb, 10Gb, or 40Gb, are all supported).

DNS Server

A DNS (Domain Name Service) server translates between a domain name (such as google.com) and an IP address (74.125.31.105). Configure the NAS to obtain a DNS server address automatically or to specify the IP address of a DNS server.

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

Note:

- Contact your ISP or network administrator for the IP address of the primary and the secondary DNS servers. We recommend set at least one DNS server to allow URL lookups.
- If you obtain the IP address by DHCP, there is no need to configure the primary and secondary DNS servers. In this case, select "Obtain DNS server address automatically".

Default Gateway

Set a network interface for the default gateway, and all out-going network traffic will go through this interface by default. To customize network routing rules, click "Static Route" > "Add" and specify the IP address/subnet and the interface for the static route. Then click "Apply".

Port Trunking

The NAS supports port trunking which combines two (or more) Ethernet interfaces into one to increase bandwidth, and to offer features like load balancing and fault tolerance.

To use port trunking on the NAS, make sure at least two LAN ports of the NAS have been connected to the same switch.

Follow these steps to configure port trunking on the NAS:

1. Go to “Control Panel” > “System Settings” > “Network” > “TCP/IP”
2. Click "Port Trunking".
3. Select two or more network interfaces to go in the trunking group
4. Select a port trunking mode from the drop-down menu. The default option is LoadBalance.
5. Click "Apply".

Note:

- For each trunking mode, you can also set its hashing method (L2:MAC address; L3:IP address; L4:port number) in the advanced settings (the pen icon next to the trunking mode).
- Make sure the Ethernet interfaces are connected to the correct switch and the switch has been configured to support the port trunking mode selected on the NAS.

The port trunking options available on the NAS:

Field	Description	Switch Required
Failover	This mode sends and receives traffic only through the master port. If the master port becomes unavailable, the next active port is used. The first interface added to the virtual interface is the master port and all subsequently added interfaces are used as failover devices. If failover to a non-master port occurs, the original port becomes master once it becomes available again.	No
LACP	The IEEE® 802.3ad Link Aggregation Control Protocol (LACP) negotiates a set of aggregatable links with the peer into one or more Link Aggregated Groups (LAGs). Each LAG is composed of ports of the same speed, set to full-duplex operation, and traffic is balanced across the ports in the LAG with the greatest total speed. Typically, there is only one LAG which contains all the ports. In the event of changes in physical connectivity, LACP will quickly converge to a new configuration. LACP balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. The hash includes the Ethernet source and destination address and, if available, the VLAN tag, and the IPv4 or IPv6 source and destination address. LACP provides greater bandwidth, redundancy and fault tolerance.	Yes
LoadBalance	The outgoing traffic is distributed according to the current load (computed relative to the speed) on each interface. Incoming traffic is received by the current interface. If the receiving interface fails, another interface takes over the MAC address of the failed receiving interface. It uses a computational algorithm to split load between the interfaces, offering increased throughput, redundancy and failover.	No

Round-Robin	Round-Robin mode is good for general purpose load balancing between two Ethernet interfaces. This mode transmits packets in sequential order from the first available slave through the last. Balance-rr provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.

VLAN

A Virtual LAN (VLAN) is a group of hosts which communicate as if they were attached to the same network switch, even if they are located in different physical locations. VLANs are used by network administrators to increase security and flexibility, and to decrease network latency and load.

To join an interface to a VLAN:

1. Go to “Control Panel” > “System Settings” > “Network” > “TCP/IP”
2. Click "VLAN", then click “Add”.
3. Specify a VLAN ID (a value between 0 and 4094).
4. Select the VLAN interface.
5. Click "Apply".

The VLAN appears in the “VLAN ID” column in the interfaces list. You can now configure the TCP/IP settings of the VLAN.

Note:

- QES supports up to 512 VLANs.
- If you need to set up both VLANs and port trunking on the same NAS, ensure to set up port trunking first, then VLANs.

IPv6

The NAS supports IPv6 connectivity with "stateless" address configurations for IPv6, RFC 2461 to allow the hosts on the same subnet to automatically acquire IPv6 addresses from the NAS. NAS services which support IPv6 include:

- CIFS/SMB
- NFS
- FTP
- iSCSI
- SNMP
- SSH

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

Service Binding

NAS services run on all available network interfaces by default. Service binding enables you to allow or block specific services from designated network interfaces to increase security. You can bind services to one or more specific network interfaces (wired or wireless). Check "Enable Service Binding" and available network interfaces on the NAS will be shown. For each service, select the network interfaces that you want bound to the service. 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.

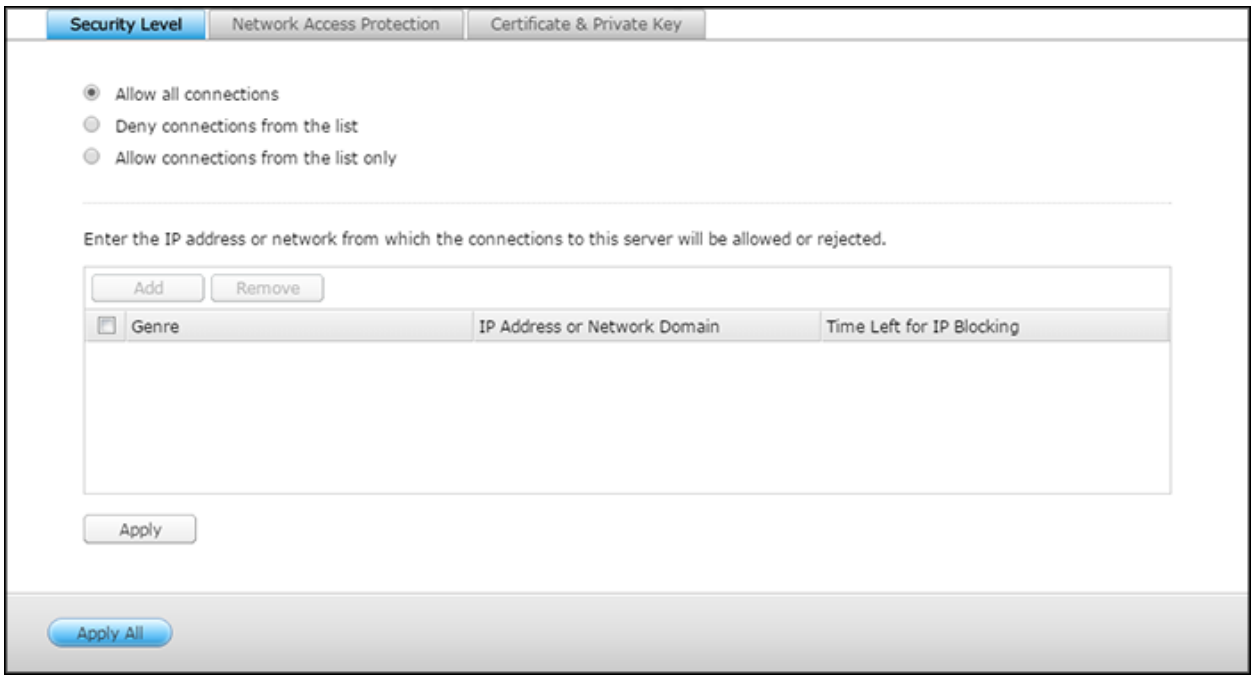
Note: After applying service binding settings, the connection of currently online users will be kept even if they were not connected to services via the specified network interfaces. The specified network interfaces will be used for the next connected session.

Proxy

Enter the proxy server settings to allow the NAS to access the Internet through a proxy server. All internet requests will go through this proxy server.

Security

Go to "Control Panel" > "System Settings" > "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 for a certain period of time or indefinitely if the IP fails to login to the NAS from a particular connection method.

Certificate & Private Key

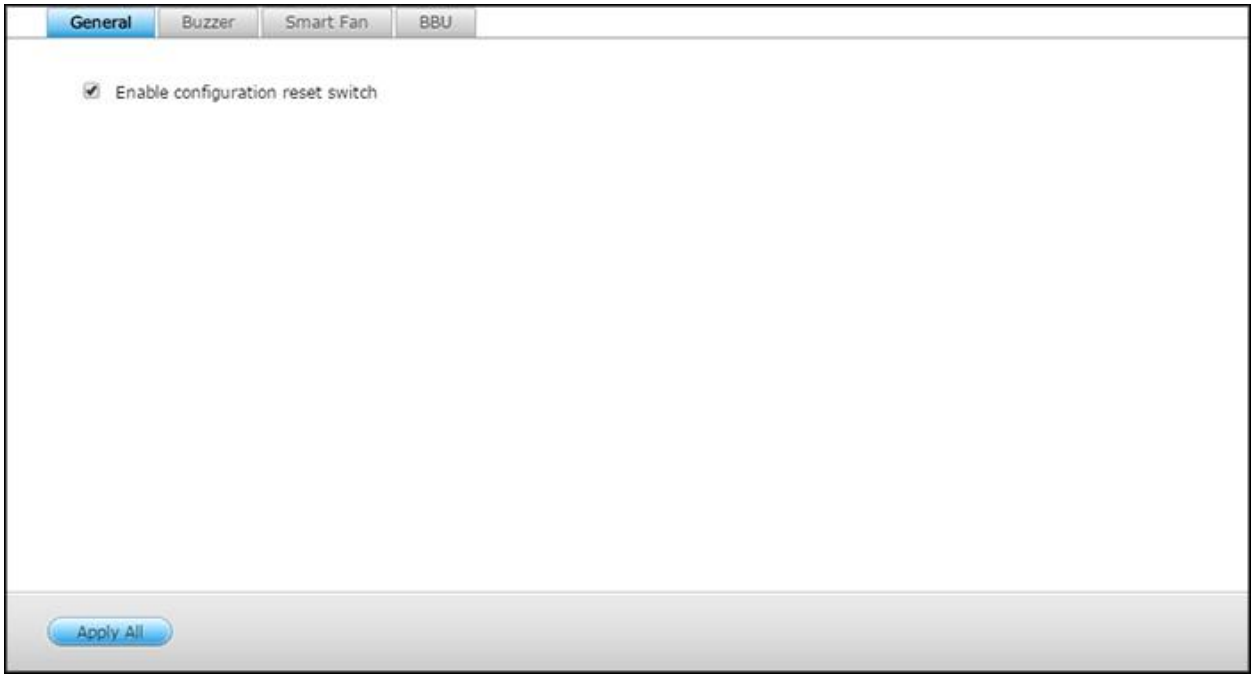
Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload an SSL certificate issued by trusted providers. After uploading an SSL certificate, users can connect to the administration interface of the NAS by SSL and there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

- 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.

Hardware

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



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: Allows all connections.
  - VLAN interfaces and IDs will be removed.
  - 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 preserved. Settings such as users, user groups, and shared folders will be cleared.

> ***Warning:***
> When performing an advanced system reset, if any system disks are also members of storage pools, then all storage pool data on those system disks will be deleted.

Buzzer

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

Smart Fan

Smart Fan Configuration:

- Enable smart fan (recommended):
  The fan rotation speed will be automatically adjusted when the NAS temperature, CPU temperature, or hard drive temperature meet the criteria. It is recommended to enable this option.
  - When ALL of the following temperature readings are met the fan will rotate at low speed:
  Select to use the default smart fan settings.
  - Self-defined temperature: Specify your own custom temperature settings for high and low fan speeds.
- Set fan rotation speed manually: The fan will constantly rotate at high, medium or low speed.

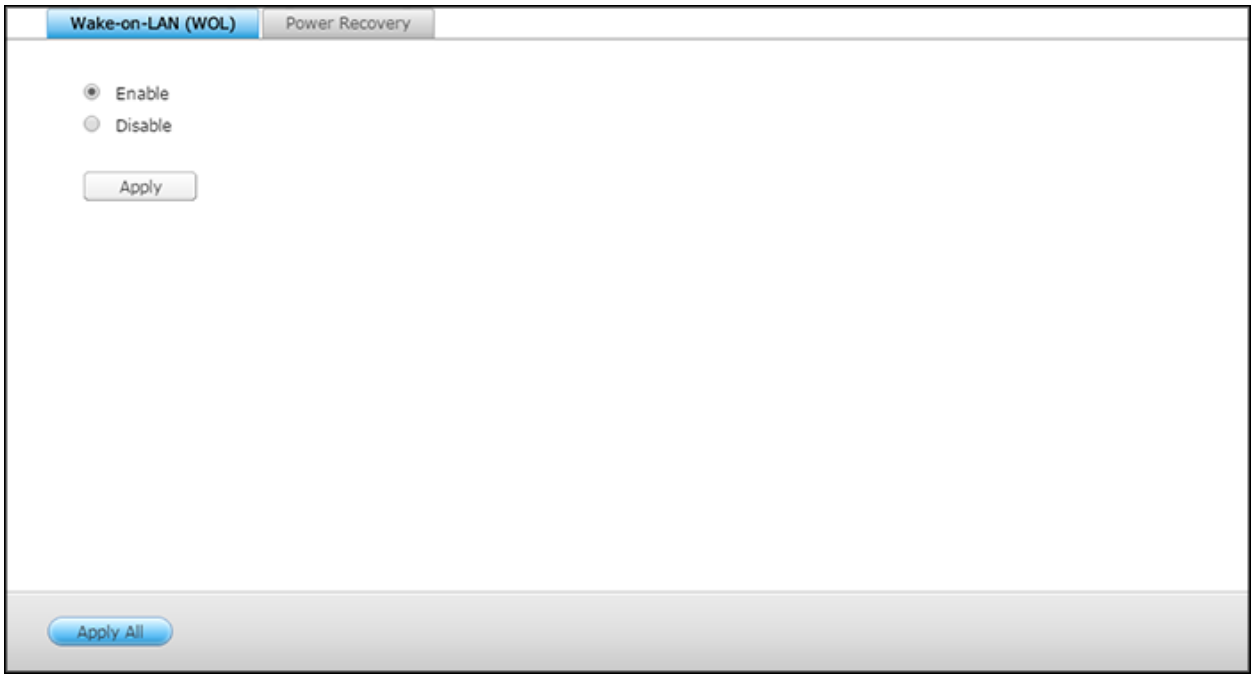
BBU

Schedule the learning cycle for the backup battery units. A learning cycle is a battery calibration operation performed by the controller to determine the condition of the battery. During this cycle, the system will switch to write-through mode to protect data integrity. It is strongly recommended to schedule the learning cycle during off-peak hours.

> **Tip:** In write-through mode, the system will write data directly into HDDs/SSDs instead of RAM first. This can avoid data loss if power outage occurs before the system finish writing data into storage from RAM when BBUs are in the learning cycle.

Power

You can configure wake-on-LAN, and specify the behavior of the NAS after a power outage.



Wake-on-LAN (WOL)

Enable this option to allow users to power on the NAS remotely by using the Wake on LAN protocol. 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 powered down, press the NAS power button or use the WOL feature in Qfinder Pro. The wake-up function on the NAS is enabled by default at "Control Panel" > "System Settings" > "General Settings" > "Power" > "Wake-on-LAN (WOL)".

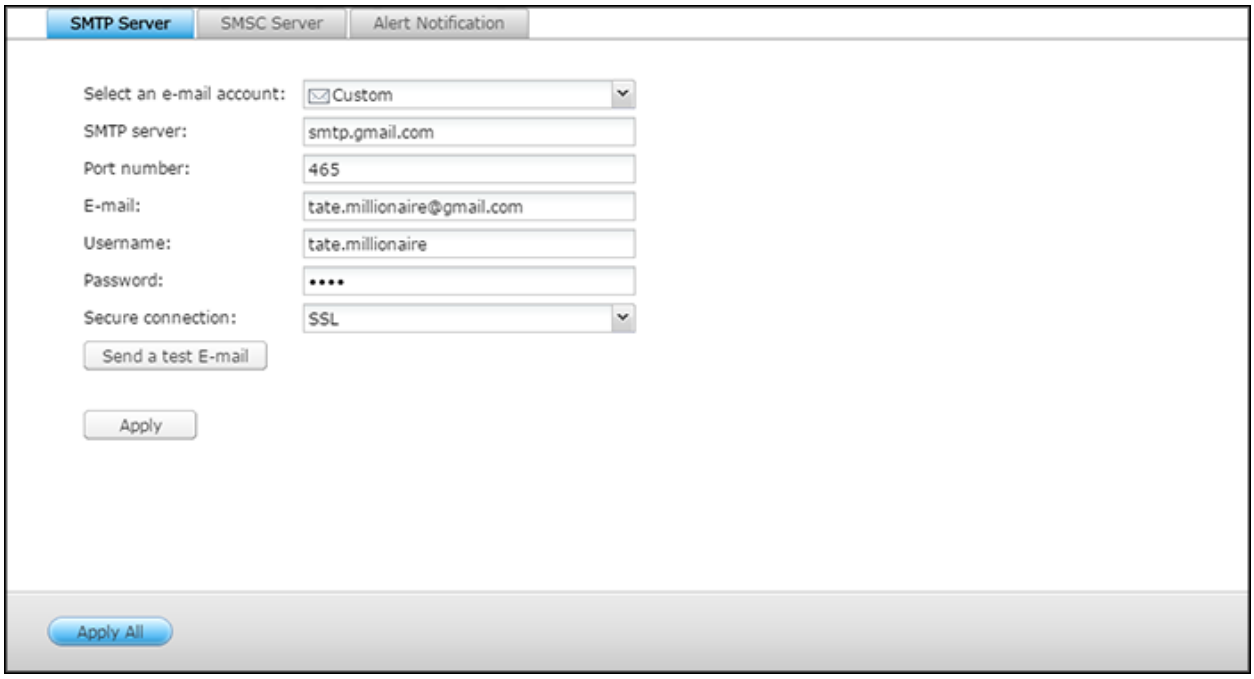
In Qfinder Pro, select a NAS and click "Tools" > "Remote Wake Up (Wake on LAN)".

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.

Notification

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



SMTP Server

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

- Select an email account: Specify the type of email account you would like to use for email alerts.
- SMTP Server: Enter the SMTP server name (for example: smtp.gmail.com).
- Port Number: Enter the port number for the SMTP server.
- E-mail: This is for testing purposes. Enter the email address of the test email recipient.
- Username and Password: Enter the credentials for SMTP server authentication. These fields are optional, leave them blank to specify no login credentials.
- Secure connection: Choose SSL or TLS to ensure a secure connection between the NAS and SMTP server or None. Enabling a secure connection is recommended if the SMTP server supports it.

SMSC Server

Configure the SMSC server settings to send SMS messages to specified phone numbers from the NAS. Follow these steps to set up an SMSC server:

1. Choose an SMS service provider. The default SMS service provider is Clickatell. You can add your own SMS service provider by selecting "Add SMS service provider" from the drop-down menu. When "Add SMS service provider" is selected, enter the name of the SMS provider and the URL template text.
2. If you choose "Clickatell", specify to enable SSL connection to the SMS service provider and fill out the server details, including the login name, login password and server API_ID.

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

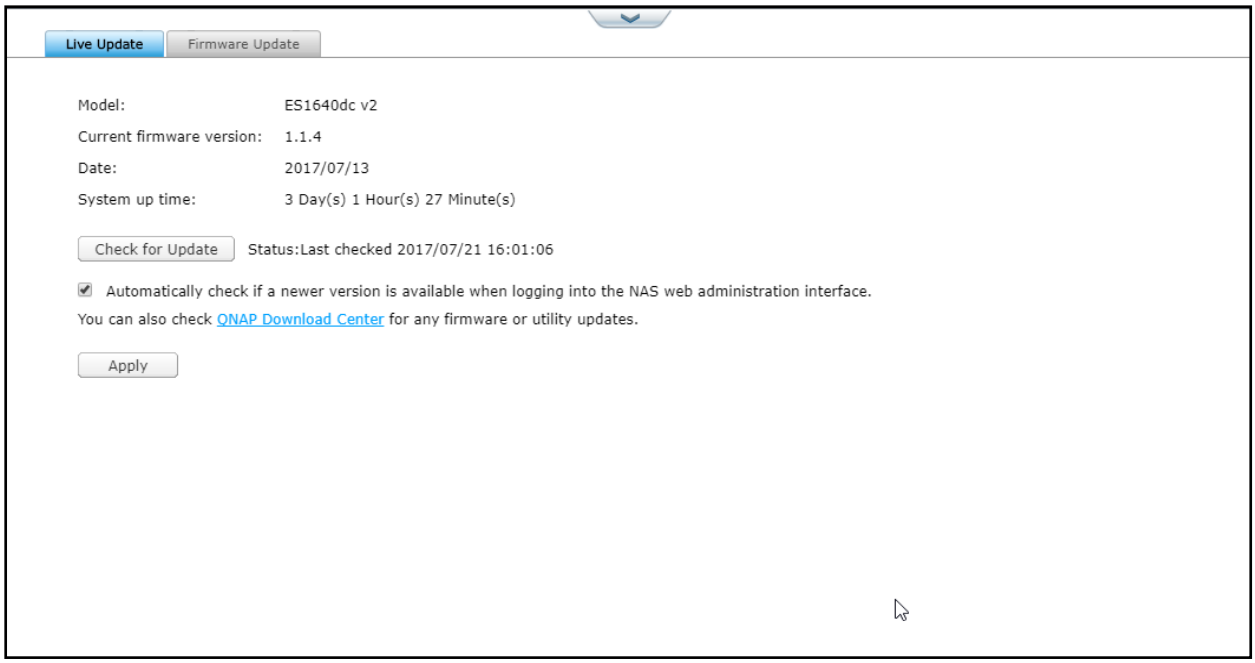
Alert Notification

Select the type of instant alerts the NAS will send when system events (warnings/errors) occur.

- Alert Notification: Specify what actions to take when a system event occurs.
- E-mail Notification Settings: Specify the email addresses (maximum 2) to receive instant system alert from the NAS.
- SMS Notification Settings: Specify the cell phone numbers (maximum 2) to receive instant system alert from the NAS.

Firmware Update

Go to "Control Panel" > "System Settings" > "Firmware Update" to update QES to a newer version.



Live Update

The NAS must be connected to the Internet with DNS correctly configured.

- Automatically check if a newer version is available when logging into the NAS web administration interface: The NAS will periodically 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.
- Check for Update: Check if a firmware update is available right now.

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, we recommend backing up all the NAS data.
4. Click "Browse" to select the firmware image for the system update. Click "Update System" to update the firmware.
5. Select the system boot option:
   - Automatically apply new firmware and restart the system after update.
   - Restart the system without interrupting services (only available on dual-controller ES NAS models): The system will pass control from the primary controller to the secondary controller.

After restarting, the system will pass control back to the primary controller. Although this process takes a longer time, it will ensure that all the services stay running.

6. Click "OK".

The system update may require a few minutes (or longer) to complete, depending on system load and storage pool utilization. The NAS will inform you when the system update is finished.

Updating Firmware using Qfinder Pro

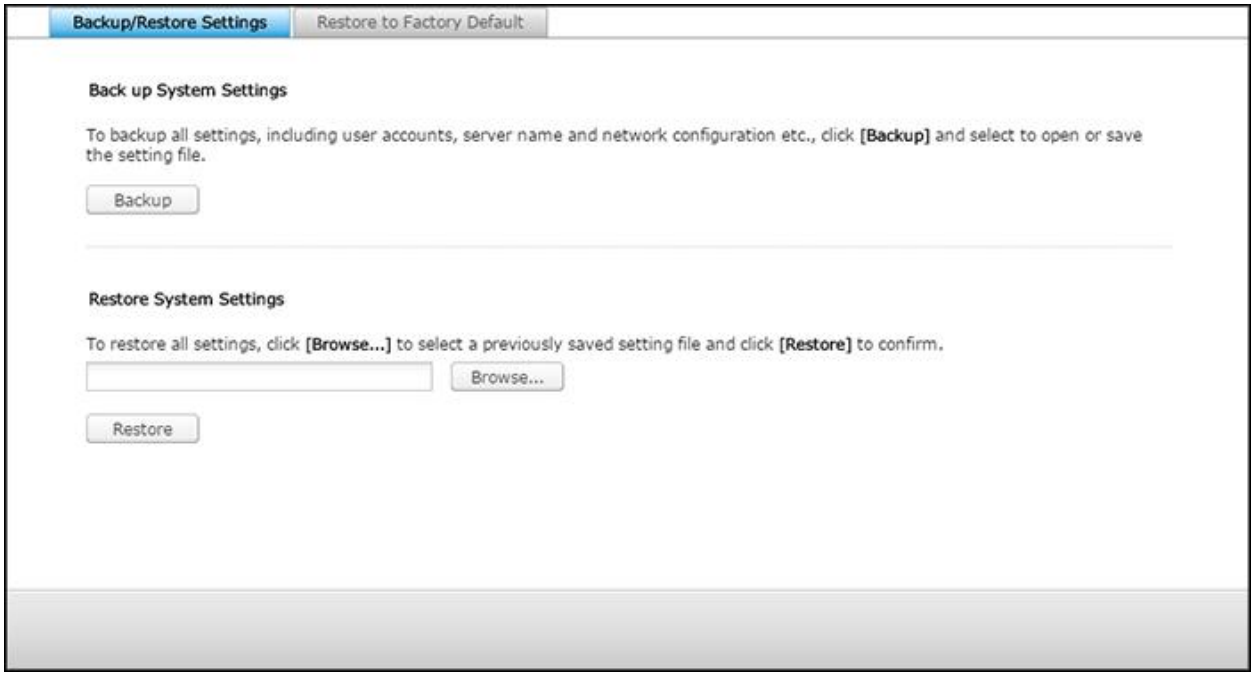
The NAS firmware can be updated using Qfinder Pro by following these steps:

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 devices on the same LAN, they can be updated at the same time with Qfinder Pro. In Qfinder Pro, select a NAS to update, then select “Tools” > “Update Firmware”. Enter the Administrator username and password, then in the “Update Firmware” window select “Update all the devices with the same model number within the network”.

Backup/Restore

Go to "Control Panel" > "System Settings" > "Backup/Restore" to back up 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 save the setting file. Settings will be backed up include: User, Group, Shared Folder, Workgroup, Domain, and LDAP, Windows File Service, NFS, 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: 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

- **Reset Settings:** Restore system settings to default without erasing user data. The following settings will be reset to the following values:
  - 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).

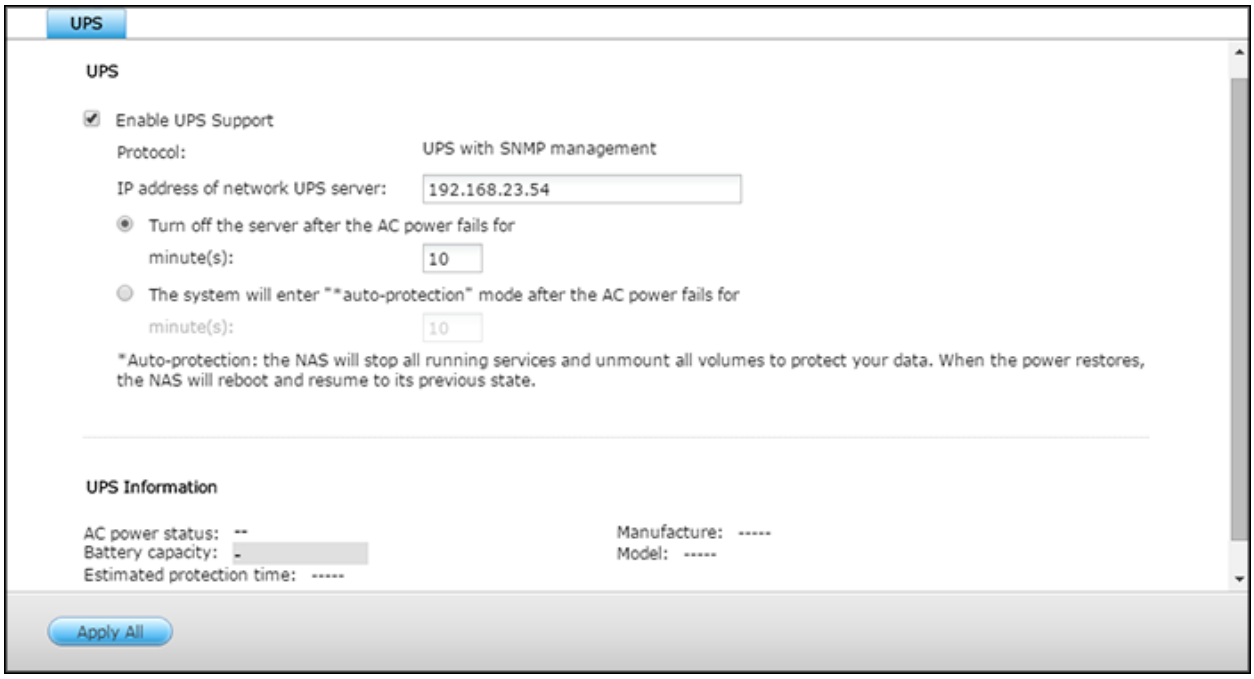
  - Security level: Allows all connections.
  - VLAN interfaces and IDs will be removed.
  - Service binding: All NAS services will be run on all available network interfaces.
- **Reinitialize NAS:** **Erases all data and system settings**.
- **Reinitialize QTS:** Switch to QTS when you are using QES. **Erases all data and system settings**.
- **Reinitialize QES:** Switch to QES when you are using QTS. **Erases all data and system settings**.

Warning: Switching to a different operating system will delete all of data stored on the NAS. Ensure that all data is backed up before switching to a different operating system.
This feature is only available on TES 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 and user groups will be cleared (but user data will be unaffected).

External Device

Go to "Control Panel" > "System Settings" > "External Storage" to configure UPS systems.



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:

- Turn off the server after the AC power fails: the NAS will shut itself down after the specified time
- Enter auto-protection mode after the AC power fails: The NAS will stop all running services to protect your data.

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, if the remaining UPS battery charge falls to less than 15%, the NAS will automatically turn itself off or enter auto-protection mode (depending on your settings) after 30 seconds regardless of the specified time in either of the above options.

In this chapter, the following topics are covered:

- **Standalone Mode – SNMP**
- **Behavior of the UPS Feature of the NAS**

Standalone Mode – SNMP

To operate under SNMP standalone mode, follow the steps below:

1. Make sure the NAS is connected to the same physical network as the SNMP-based UPS.
2. Select the option "Enable UPS Support".
3. Enter the IP address of the SNMP-based UPS.

4. 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.
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. All shared folders and iSCSI LUNs 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:

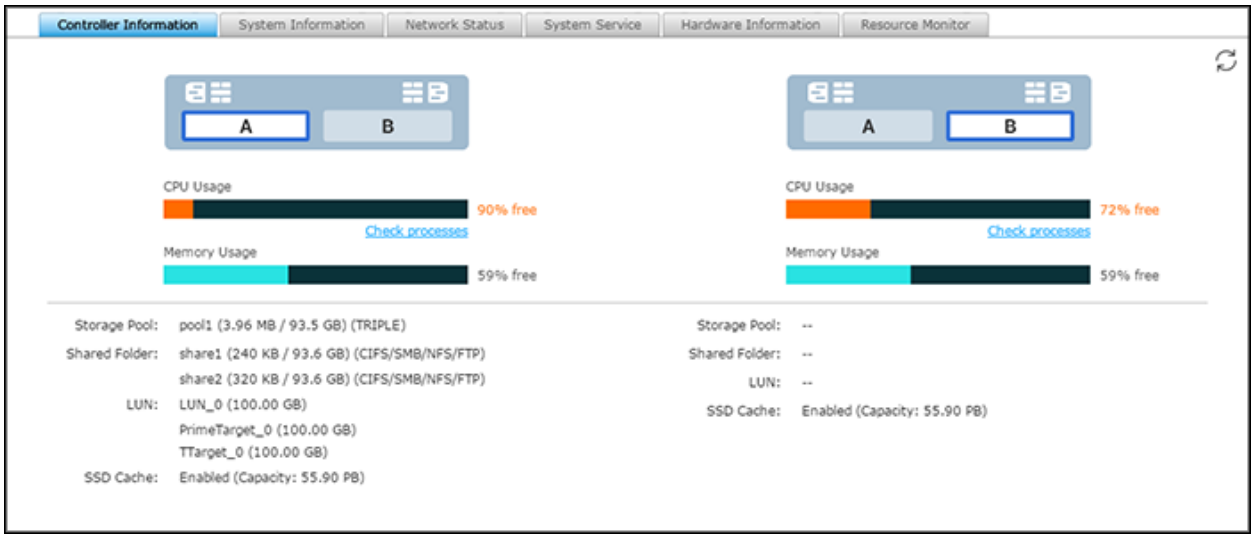
Depending on your setting on the "UPS" page:

- 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" > "Power Recovery".

System Status

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



Controller Information

View the summary of controller information (such as CPU and RAM usage, storage usage of the storage pools, shared folders and LUNs) for each controller. Click "Check Processes" under "CPU Usage" to check the processes the controller is currently running.

System Information

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

Network Status

View the current network settings and statistics on this page. They are displayed based on network interfaces. Click the "-" in the top left to collapse the interface page and the "+" to expand it.

System Service

View the current status of system services, such as Microsoft networking, NFS, FTP and File Station.

Hardware Information

View basic NAS hardware information, such as CPU usage, memory, cache and system fan speed.

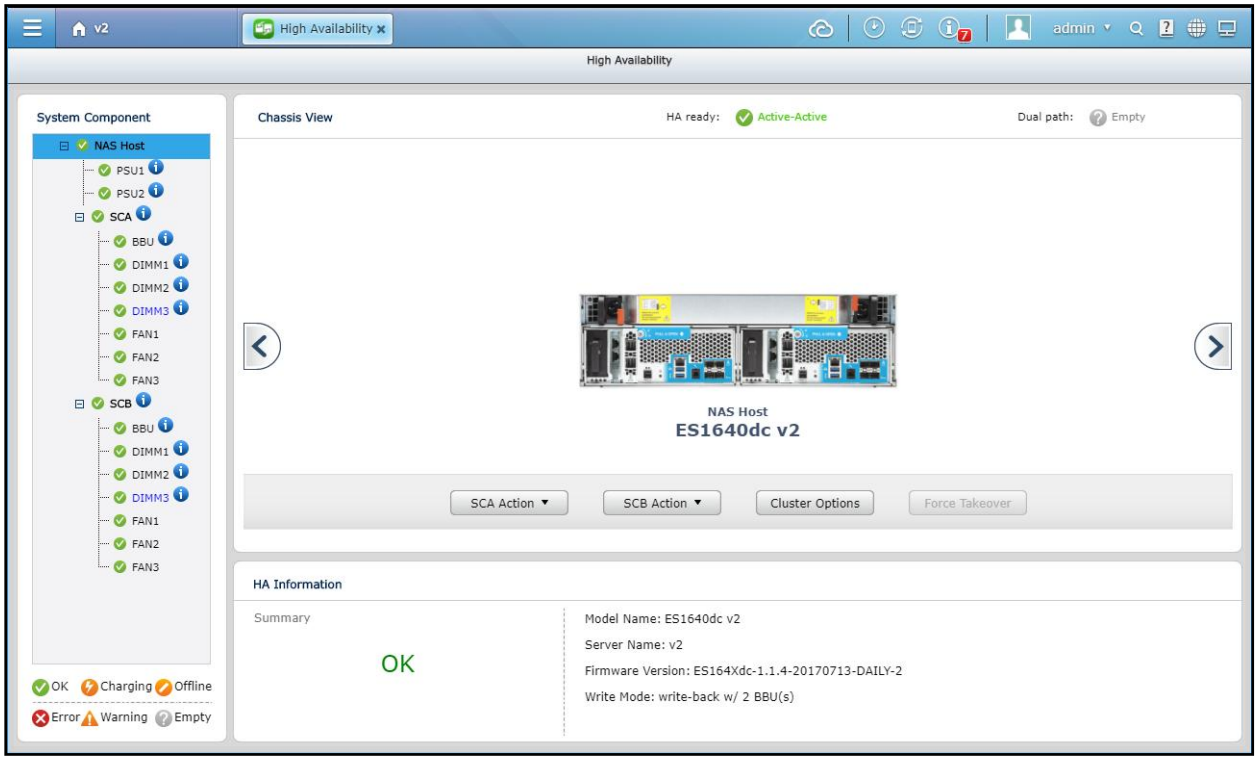
Resource Monitor

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

- CPU Usage: Shows the CPU usage of the NAS.
- Memory Usage: Shows the memory usage of the NAS by real-time dynamic graph.
- SSD Cache: Shows the SSD cache usage and the hit rate history.
- Disk Usage: Shows the disk space usage of each storage pool, shared folder and LUN.
- Network Usage: Provides bandwidth transfer information of each available NAS interface.
- Process: Shows information about the processes running on the NAS.
- Disk Performance: Shows IOPS and throughput of the selected pool.

High Availability

High Availability is the dashboard in QES for monitoring the status of each system component and managing controllers to ensure sustainable system availability for mission critical applications. To launch and configure High Availability, go to "Control Panel" > "System Settings" > "High Availability" or directly click the "High Availability" shortcut on QES desktop.



Note: High Availability is only available on dual-controller NAS models.

Monitoring System Components

Click "+" beside a NAS host or expansion enclosure in "System Component" to check its components and their general information. Check the table below for a list of system components and their available information:

Component	Available Information
NAS host	Model name, server name, firmware version, write mode.
Expansion enclosure (REXP)	Model name.
NAS Host Controller (SCA/SCB)	Host name, machine status, initialization status
Expansion enclosure Controller (ECA/ECB)	Machine status
Power supply unit (PSU)	Model, power, temperature, fan speed. (For expansion enclosures: Only temperature, fan speed.)
Backup battery unit (BBU)	Capacity, temperature, voltage, serial number, date manufactured, date initialized.
DIMM (RAM)	Manufacturer, type, serial number, size, speed.
FAN	Mode, speed. (For expansion enclosures: Only fan speed.)

The legend shown under the system component panel is provided to indicate the status of the chosen component.

- OK: The component is functioning properly.
- Charging: The battery is charging now.
- Offline: The component is not detected by the system.
- Error: The component is detected with errors and is recommended to be replaced immediately.
- Warning: The component is approaching failure.
- Empty: The component is missing or not installed.

Observing System Availability Status

On top right side of the window, there are two status indicators for system high availability and expansion enclosure connection status.

"HA ready" shows the current state of controllers. There are four possible states:

- Active-Active: Both controllers on the NAS are functioning properly.
- Taking over: The remaining active controller is in the process of taking over for another controller.
- Takeover: The system is now controlled only by the active controller.
- Giving back: The controller that took over previously is now returning control back to the recovered controller.

"Dual Path" shows the status of connection between the NAS and expansion enclosures. There are three possible states:

- Dual Path: The expansion enclosure is connected to the NAS in a dual path.
- Single Path: The expansion enclosure is currently detected connecting to the NAS in a single path.
- Empty: No expansion enclosures are currently connected to the NAS.

Note: For details on connecting a NAS and an expansion enclosure, see the hardware user manual.

Using Controllers for Failback Operations and Configuring Cluster Options

You can manually use controllers to perform failback operations (such as takeover and giveback), manage the controllers (such as restart, shutdown or power on), and configure the controller cluster for failback settings. Refer to the following table for details:

Action	Description
Takeover (under "SCA Action" or "SCB Action")	When SCA takes over, services will bind to controller SCA. Controller SCB will go into standby mode and won't provide network services anymore.
Giveback (under "SCA Action" or "SCB Action")	When controller SCA gives back, services bind to controller SCB. SCB will then become active mode and start providing network services.
Restart (under "SCA Action" or "SCB Action")	Click this button to restart the controller.
Shutdown (under "SCA Action" or "SCB Action")	Click this button to shut down the controller.
Power On (under "SCA Action" or "SCB" Action)	Click this button to power on the controller.

Cluster Option	Click this button to configure failover settings for the controller cluster. Available options include:
	• System failover protection:
	  ○ Failover when network fails: When a controller becomes inaccessible as a result of network connection failure, the other controller will automatically take over.
	  ○ Failover when JBOD failed: When the expansion enclosures connected to a controller become inaccessible, the other controller will automatically take over.
	• Automatically failback when system recovered: Enable this option and the recovered controller will automatically regain control from the controller that previously took over.
	  • Prevent failback repeatedly: In some instances, failback operations fail and the recovered controller persistently attempts to regain control from another controller. When this happens, the HA ready status is "Takeover". You can confirm the status when you check the Event Notifications and System Logs.
	  To avoid this scenario, enable “Prevent failback repeatedly” to force the recovered controller to attempt failback twice (once every 30 seconds) before temporarily disabling automatic failback for 24 hours. During this 24-hour period, the user can select "Giveback" on the “Takeover” controller to manually failback, and re-enable automatic failback.
	  For more details, see the Automatic Failover Lock section below.
	• Management port failover: Enable this option and when the management interface of one controller fails, another controller will take over. Note that the management interfaces of both controllers must use static IP addresses or the option will be disabled. To set a static IP, go to "Control Panel" > "System Settings" > "Network".

Force Takeover	The recovered controller should regain control automatically, but in some cases this may not happen. You can click this button to force the recovered controller to regain control. This button is only available after "Takeover" under the controller is disabled.

Automatic Failover Lock

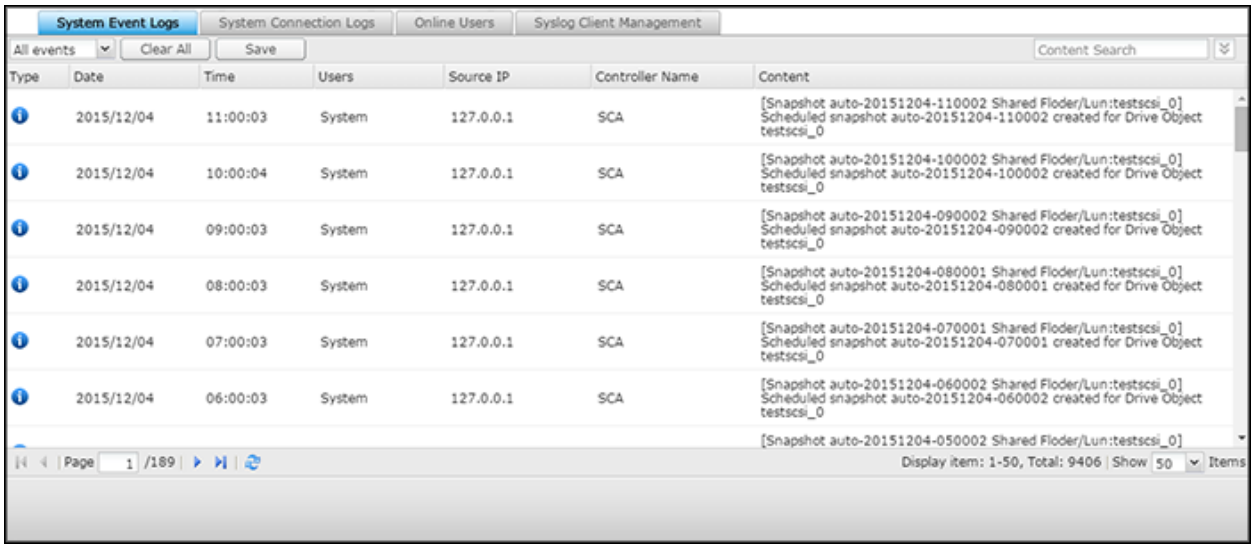
Enabling the “Prevent failback repeatedly” option also enables the automatic failover lock mechanism. To enable this setting, go to “Cluster Options” > “Automatically failback when system recovers” and then select “Prevent failback repeatedly”.

By default, the failover status is unlocked. However, when an automatic failover happens and automatic failback occurs, the status changes to "Lock until XXXX-YY:YY".

If no other failover occurs in the next 24 hours, the status reverts to “Unlocked”. However, if another failover happens, the status changes to “Locked”. Users will then need to manually click “Giveback” from the action menu of the “Takeover” controller to pass the control back to the “Standby” controller. This step also unlocks the system and removes the 24-hour countdown.

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.

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

System Connection Logs

The NAS can record HTTP, FTP, SSH, SMB, and iSCSI connections. Click "Options" to select the connection type to be logged. File transfer performance may be slightly impacted when this feature is enabled. You can also choose to archive connection logs and save the file in a folder when the number of logs reaches 10,000.

> **Tip:** Right click on a record and select to delete the record or to block the IP and select how long the IP should be blocked. To clear every log, click "Clear All".

Start Logging: Enable this option to archive connection logs. When the number of logs reaches the upper limit the NAS will automatically generate a CSV file and save it to a specified folder. File-level access logs are available on this page. The NAS will record logs when users access, create, delete, move, or rename any files/folders via the connection type specified in "Options". To disable this feature, click "Stop logging".

> **Note:** For SSH connections, the system can only record login and logout events.

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. To use advanced search:

1. Go to "Control Panel" > "System Settings" > "System Logs" > “System Event Logs”.
2. Click  next to the search bar at the top-right of the window.
3. Specify the log type, users, controller name, date range and source IP.
4. Click "Search".

myQNAPcloud Service

myQNAPcloud provides host name registration, mapping of a dynamic NAS IP to a domain name, and auto port mapping for UPnP routers on the local network. Use the myQNAPcloud wizard to register a unique host name for the NAS, configure automatic port forwarding on the UPnP router, and publish NAS services for remote access over the Internet.

To use the myQNAPcloud service, make sure the NAS has been connected to an UPnP router and the Internet and click "Control Panel" > "System Settings" > "myQNAPcloud".

This chapter includes two parts:

- myQNAPcloud Wizard
  - My DDNS

myQNAPcloud Wizard

It is recommended to use the wizard the first time you use myQNAPcloud. Follow these steps:

1. Click "Get Started" to use the wizard.
2. Click "Start".
3. Fill out your myQNAPcloud ID (QID) and password. If you don’t already have an account, click "Create myQNAPcloud account" to sign up. Click "Next".
4. Enter a name to register your NAS and click "Next".
5. Select to enable the myQNAPcloud services (Auto Router Configuration, myQNAPcloud device name (DDNS). Click "Finish".

After account login, you can click "Manage myQNAPcloud Account" to manage your account on the myQNAPcloud portal site or click "Sign out" to sign out your account.

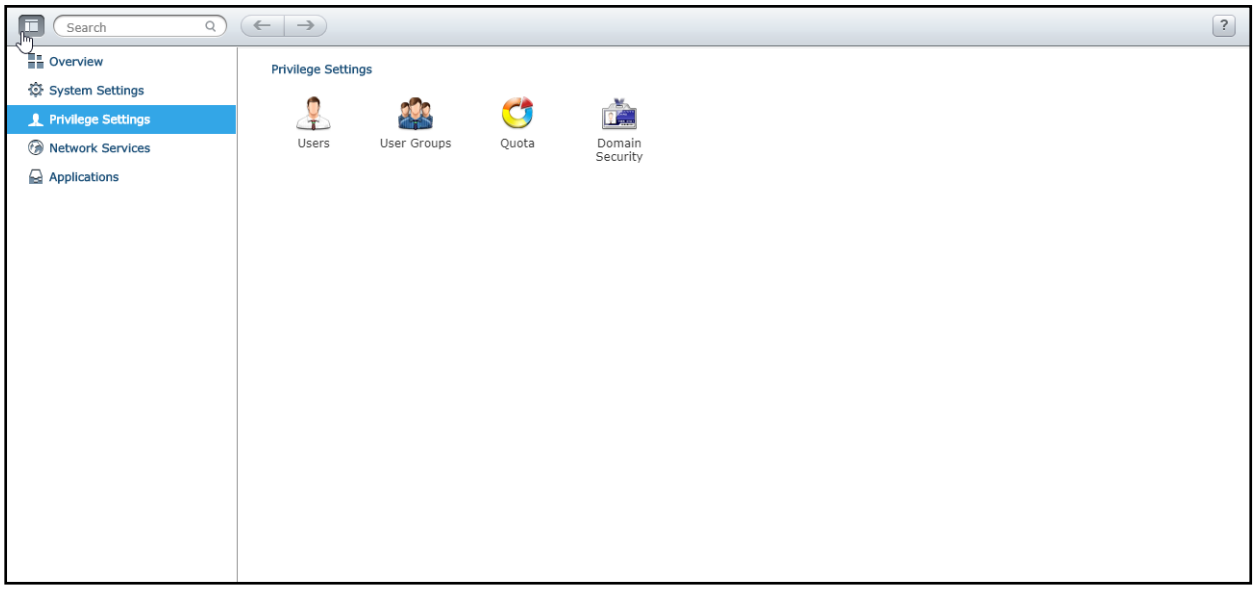
My DDNS

By enabling the myQNAPcloud DDNS service, you can connect to the network services on your NAS by using your specified Internet address. To change your myQNAPcloud DDNS domain name, click the "Here"

link on the page. Your recent DDNS information will be shown here and you can click the "Update" button to refresh the result.

Privilege Settings

Go to "Control Panel" > "Privilege Systems" to configure privilege settings, disk quotas and domain security on the NAS.

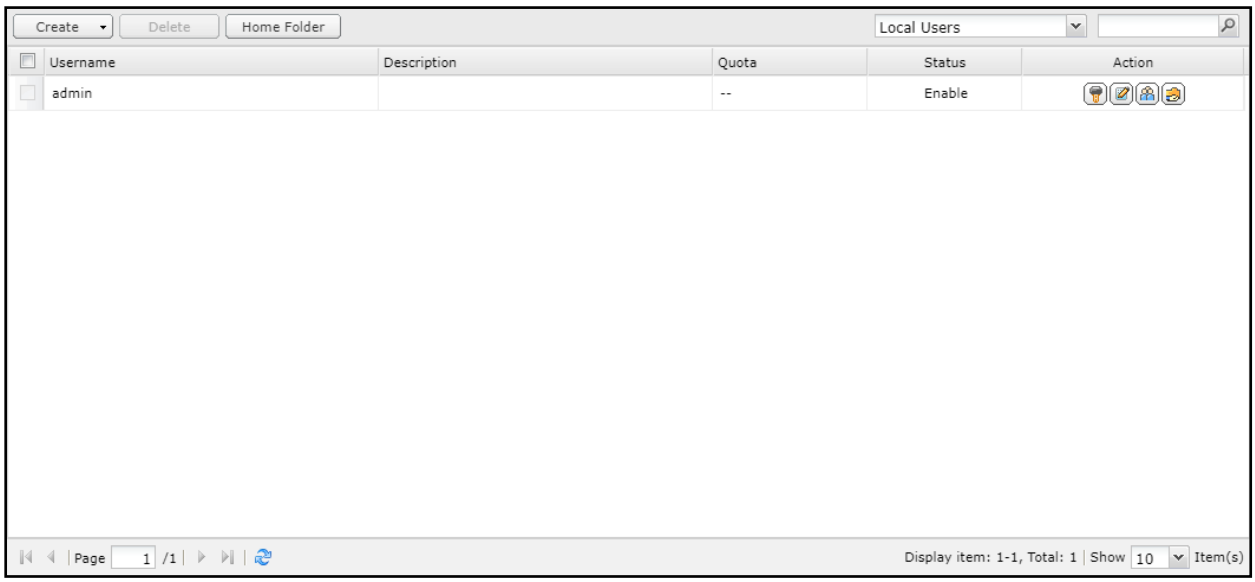


For setup details, refer to the following links:

- Users
- User Groups
- Quota
- Domain Security

Users

On this page, you can create, import/export and manage user accounts.



In this chapter, the following topics are covered:

- Default User Accounts
- Creating Users
- Importing/Exporting Users
- Managing Users
- Home Folders

Default User Accounts

The administrator "admin" default account has full access to system administration and all shared folders. It cannot be deleted but it can be disabled. To disable the built-in admin account, first add another user account to the administrators group. Then log in as this user account to disable the build-in admin account.

Creating Users

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. The password length must be 5 to 64 characters.

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. Fill out the required fields, edit the user group this user belongs to, specify the shared folder permission and edit application privileges. Click "Create".

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 a name prefix, starting number, and the number of users.
   Example:
   Name prefix: test
   Starting number: 1
   Number of users: 5
   QES creates five users with the following user names: test1, test2, test3, test4, and test5. The password is the same for all five users.

Note: QES removes leading zeros in starting numbers. For example, "001" becomes "1".

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 first 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.

   Example TXT import:

```
John,s8fk4b,30,Sales
Jane,9fjwbx,40,Marketing
Mary,f9xn3ns,10,RD
```

Note: If the quota field is set to 0, then the user will have no quota limit.

CSV (Excel)

1. Open a new file with Excel.
2. Enter a user's information in the same row in the following order:
   - Column A: Username
   - Column B: Password
   - Column C: Quota (MB)
   - Column D: Group name
3. Go to the next row and repeat the previous step to create another user account. Each row indicates one user's information. Save 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.

Example of a CSV file:

	A	B	C	D
1	John	s8fk4b	30	Sales
2	Jane	9fjwbx	40	Marketing
3	Mary	f9xn3ns	10	RD

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".

Managing Users

After you create or import users, you can modify their user settings by clicking the following action icons in the "action" column.

Action	Description
Change password	Change the users password
Edit account profile	• Modify email, phone number and description information • Disable this user account **Note**: To disable the built-in admin account, first add another user account to the administrators group. Then log in as this user account to disable the build-in admin account.
Edit user groups	Add or remove this user from different user groups
Edit shared folder permissions	Allow read/write access, read-only access, or deny access to each shared folder on this NAS.
Edit application privileges	Allow or disallow access to QES applications. For example, File Station.

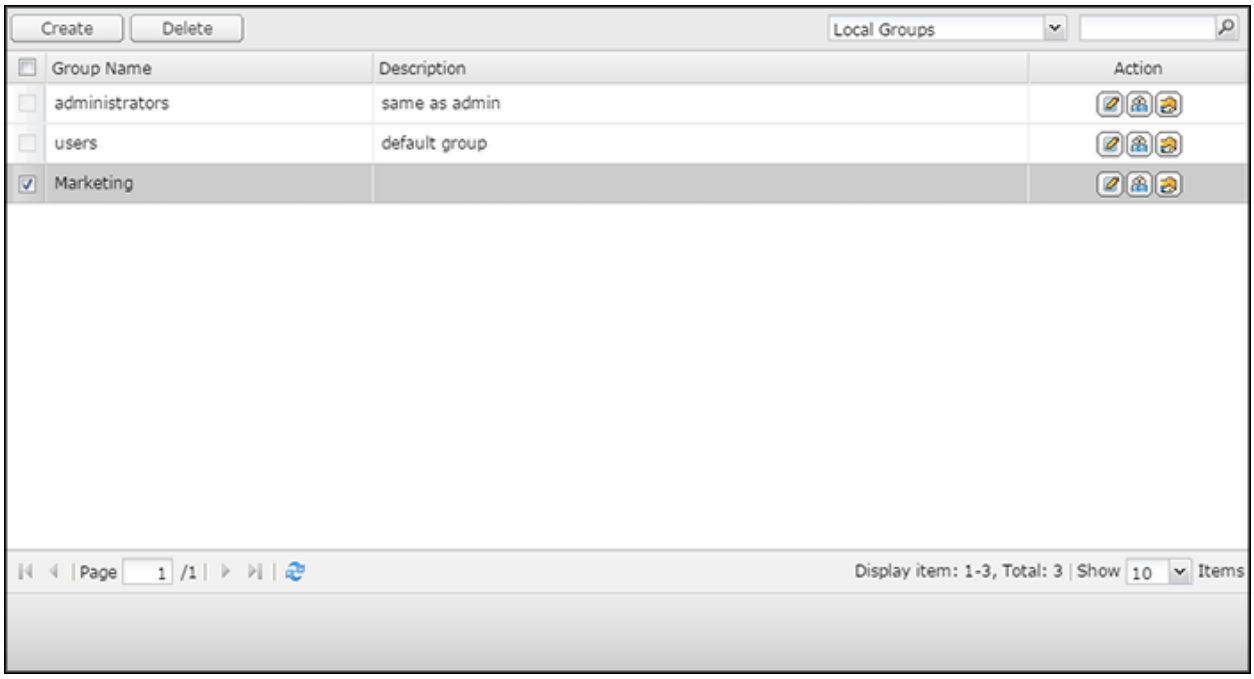
Home Folders

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" or members of the "administrators" group by default.

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

User Groups

On this page, you can create and manage 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.
- Users: All the registered users belong to this group. This group cannot be deleted.

A group name cannot exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones: " / \ [ ] : ; | = , + * ? < > ` '

Creating User Groups

To create a user group on the NAS, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "User Groups".
2. Click "Create".
3. Fill out the required fields, assign users to the group and edit the shared folder permission. Click "Create".

Managing User Groups

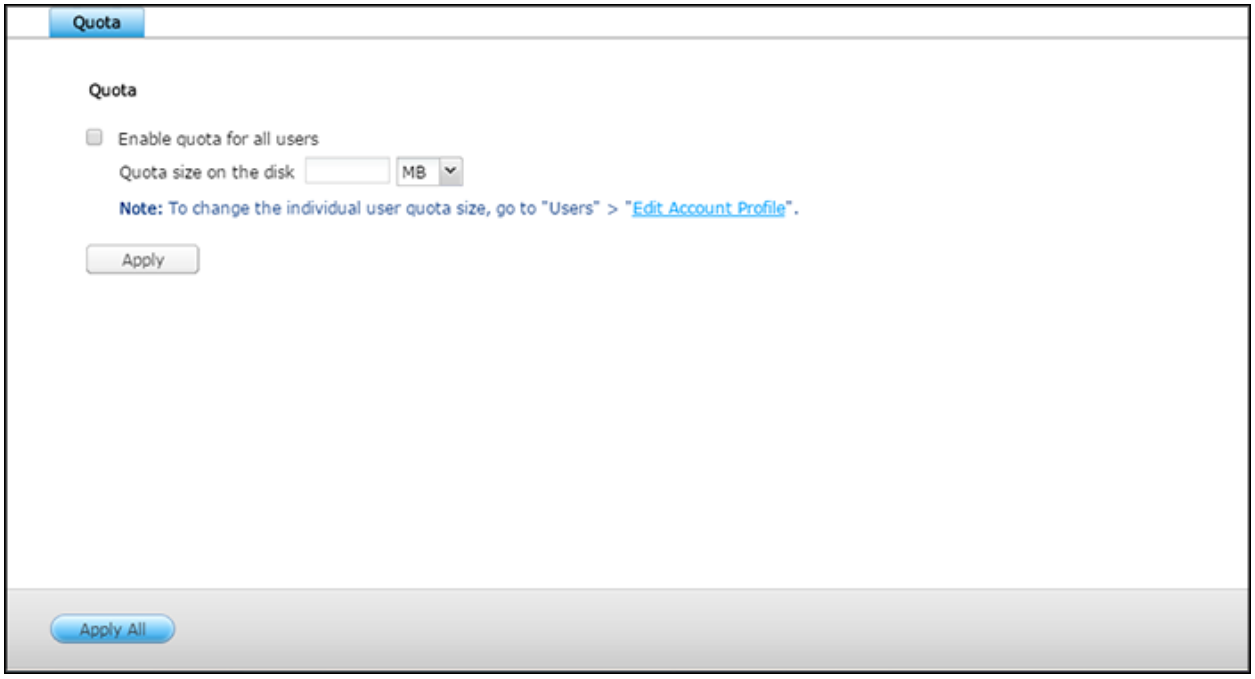
After you create user groups, you can edit their group details, group users, and shared folder access rights. To do so, click the corresponding button under "Action" for the group name. To delete a user group, follow these steps:

1. Go to "Control Panel" > "Privilege Settings" > "User Groups".

2. Select a group name.
3. Click "Delete".

Quota

To efficiently allocate storage space, you can specify quotas that can be used by each user. When this is enabled and a user has reached the quota, the user cannot upload any more data to the NAS.



By default, no limitations are set for the users. You can modify the following options:

- Enable quota for all users
- Quota size on the disk

After enabling the quota setting for all users and specify the quota size, the quota settings will be shown. Click "Generate" to generate a quota settings file in CSV format. After the file has been generated, click "Download" to save it.

Note: You can also set a different quota size for individual users in "Control Panel" > "Privilege Settings" > "Users" > "Edit Account Profile".

Domain Security

The NAS supports user authentication by local access right management, Microsoft Active Directory (Windows Server 2003/2008/2012), 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.

The following settings are available:

- **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
  - FTP
  - File Station
  - NFS

- **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. Both the local NAS users and LDAP users can access the NAS via the following protocols/services:
  - Samba
  - FTP
  - File Station
  - NFS

Joining the NAS to Active Directory (Windows Server 2003/2008/2012/2016)

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 that centrally holds information for users, user groups, and computers for secure access management. The NAS supports Active Directory (AD). By joining the NAS to the Active Directory, all of the AD server's user accounts will be automatically imported to the NAS. AD users can use the same login details to access the NAS. When joining a domain controller, connect both management ports of each controller to the network switch if you are using a dual-controller ES NAS (ES1640dc or ES1640dc v2).

Joining the NAS to Active Directory 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 "System Settings" > "General Settings" > "Time". Set the date and time of the NAS, which must be consistent with the time of the AD server. The maximum time disparity tolerated is 5 minutes.
2. Go to "System Settings" > "Network" > "TCP/IP". Set the IP of the primary DNS server as the IP of the Active Directory server that contains the DNS service. It must be the IP of the DNS server that is used for your Active Directory. If you use an external DNS server, you will not be able to join the domain.
3. Go to "Privilege Settings" > "Domain Security". Enable "Active Directory authentication (domain member)", and click "Manual Configuration".
4. Specify the following AD information:

Field	Example Data	Details
Domain NetBIOS Name:	qnap	
AD Server Name	dc1	
Domain	qnap.com	
Domain Administrator Username	admin	The AD user entered here must have administrator access rights to the AD domain.
Domain Administrator Password	password123	
Organization Unit (Optional):	computers	OU that the NAS will go in.
Server Description (Optional):	QNAP ES1652DC NAS	Used by the NAS SAMBA service in the server's "Comment" field. You will see this description when connecting to a NAS samba share using the command line interface.

Note: If you are using a WINS server on the network and workstations are configured to use that WINS server for name resolution, you must set up the WINS server IP on the NAS.

To use a WINS server, go to “Control Panel” > “Network Services” > “Win/NFS” > “Microsoft Networking” > “Advanced Options”, enable "Use the specified WINS server", specify an IP and click “Apply”.

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

To use the AD Quick Configuration Wizard, follow these steps:

1. 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 domain name of the domain name service (DNS). The NetBIOS name will be automatically generated when you enter the domain name. Specify the DNS server IP for domain resolution. The IP must be the same as the DNS server of your Active Directory. Click "Next".
4. Select a domain controller from the drop-down menu. The domain controller is responsible for time synchronization between the NAS and the domain server and user authentication. Enter the domain administrator name and password. Click "Join".
5. 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.

Windows Server 2003

The AD server name and AD domain name can be checked in "System Properties" in Windows. As an example, for Windows Server 2003, if you see "node1.qnap-test.com" as the "Full computer name" on the system properties dialog window, the AD server name is "node1" and NOT "node1.qnap-test.com" and the domain name remains the same as qnap-test.com.

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.

Windows Server 2012 and 2016

To check the AD server name and domain name, right-click on the Windows start button, then click “System”. 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, to log into the NAS and access NAS shared folders:
  - Local NAS users must use "NASname\NASusername"
  - AD users must use “Domain\DomainUsername”

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 reload 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.

Trusted Domains

A trusted domain is a domain that an active directory domain trusts to authenticate users. If the NAS is added to an active directory domain, then all users from trusted domains can also be used to log into the NAS and access shared folders. Trusted domain users and groups can also be used when setting shared folder permissions. By default, this feature is disabled in QES.

To enable trust domains

1. Go to Control Panel > Network Services > Win/NFS > Microsoft Networking > Advanced Options.
2. Select "enable trust domains".
3. Click apply.

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 devices with the same login details. This feature is intended for use by administrators and users who have knowledge of FreeBSD 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 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.

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

6. When the NAS is connected to an LDAP server, the administrator can:
   - Go to "Privilege Settings" > "Users" and select "Domain Users" from the drop-down menu. The LDAP users list will be shown.
   - Go to "Privilege Settings" > "User Groups" and select "Domain Groups" from the drop-down menu. The LDAP groups will be shown.
   - 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. 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 FreeBSD server where the LDAP server is running (it can be different depending on the FreeBSD 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
```

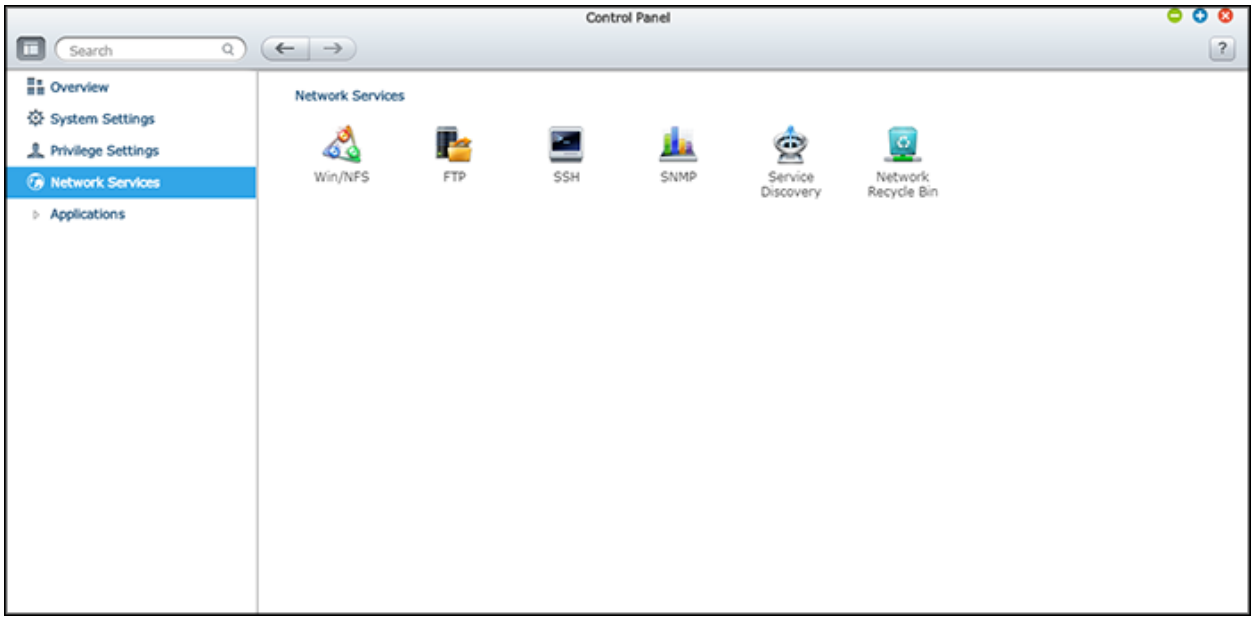
Configuration examples

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

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

Network Services

Go to "Control Panel" > "Network Services" to configure network services on the NAS.



For setup details, refer to the following links:

- Win/NFS
- FTP
- SSH
- SNMP Settings
- Service Discovery
- Network Recycle Bin

Win/NFS

Go to "Control Panel" > "Network Services" > "Win/NFS" to configure networking services.

In this chapter, the following topics are covered:

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

- **Use the specified 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 Master Domain:** This option assigns the NAS the role of Local Master Browser on its network. A Local Master Browse which is responsible for maintaining a list of all computers on the network, that are in the same workgroup. The name of the NAS workgroup must be the same as that of your computer's workgroup (the default in Windows is "workgroup"). The setting is enabled by default. If you disable it, the NAS will not maintain the computer list, and the job will be done by another computer on the network.
- **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 resolve 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.
- **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 "Control Panel" > "Privilege Settings" > "Users" > "Action" > "Edit Shared Folder Permissions". Users from trusted domains can also be added to groups at "Control Panel" > "Privilege Settings" > "User Groups". Domain trusts are only set up in Active Directory, not on the NAS.
- **Enable Asynchronous I/O:** Enable this option to speed up the SAMBA performance, but an UPS is strongly recommended to prevent power interruption if this option is to be enabled.
- **Force Encryption Transport:** Set the folder to be accessible for SMB 3 clients. After it is enabled, all communications via Microsoft Networking will be conducted via SMB 3 and encrypted. All SMB 3 clients will be able to connect to NAS via Microsoft Networking.

- **Highest SMB version:** Choose the version of the SMB protocol (Server Message Block) from the drop down list for your Microsoft Networking operations. If you are not sure, please use the default one on the list.

NFS Service

To connect to the NAS from Linux/FreeBSD, enable the NFS service. To configure NFS access rights to shared folders on the NAS, refer to the NFS host access section for details.

Connecting to the NAS by NFS
On Linux/FreeBSD, run this command:

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

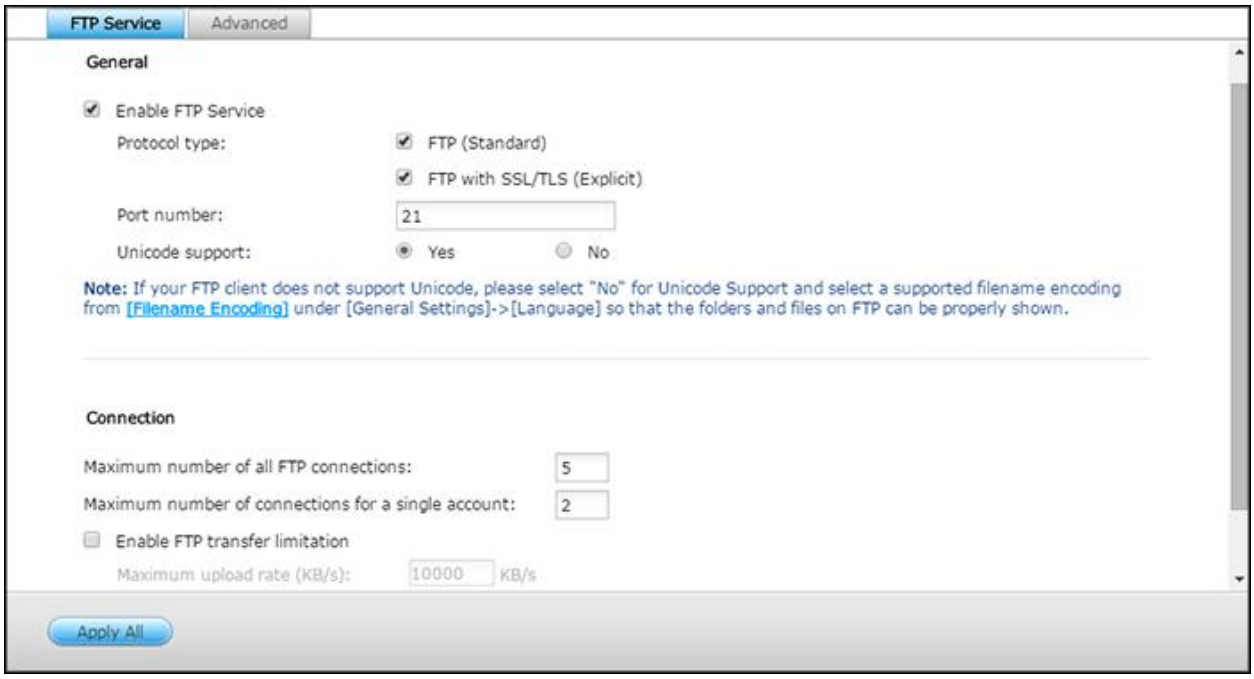
For example, if the IP address of your NAS Ethernet interface is 192.168.0.1 and you want to link the shared folder "public" under the /mnt/pub directory, use this command:

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

Note: You must login as "root" or as a user with root permissions to use the above command.

FTP

Go to "Control Panel" > "Network 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. Then connect to the NAS using an FTP client such as FileZilla.

- **Protocol Type:** Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the correct protocol type in your FTP client to ensure successful connection.
- **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 "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.
- **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.

Note: The maximum number of concurrent FTP connections is 1024.

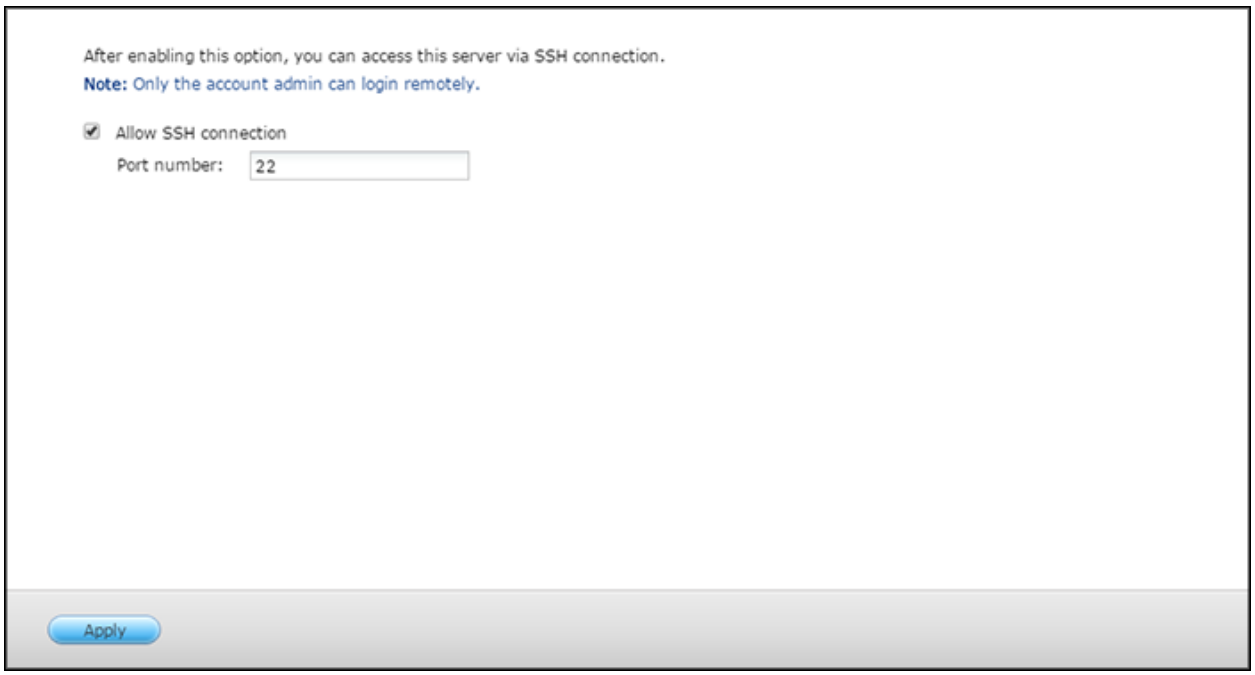
Advanced

- **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.

SSH

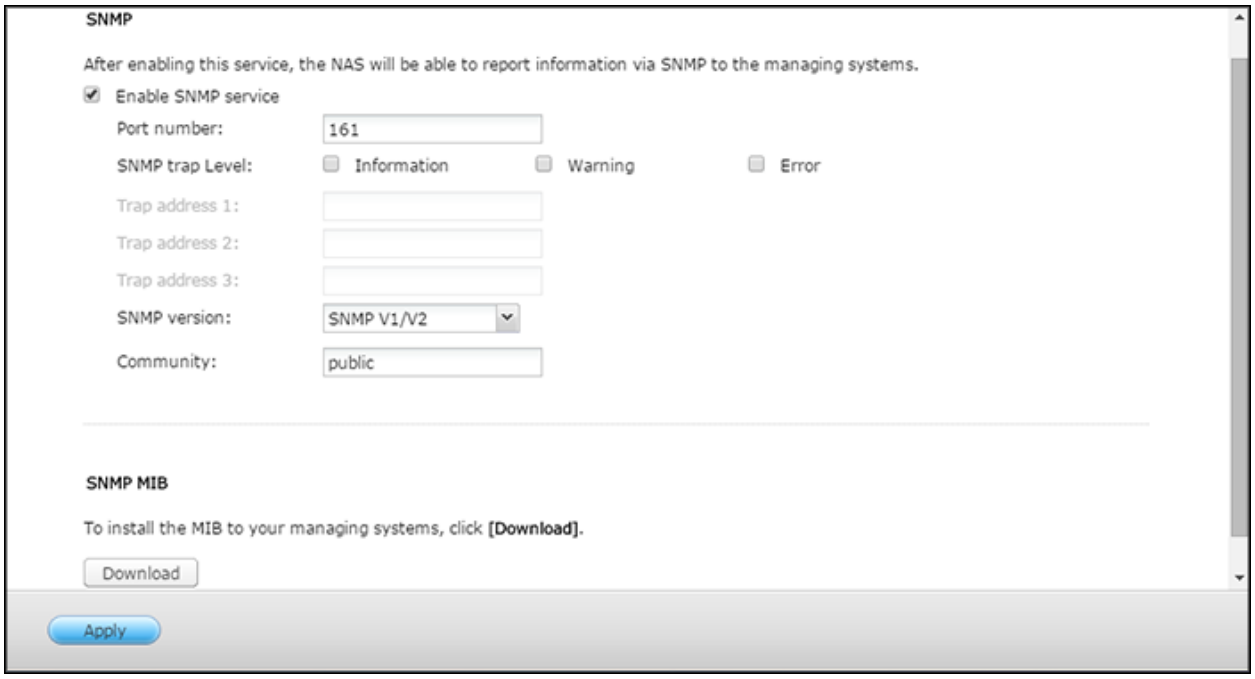
Enable this option to connect to the NAS by SSH encrypted connection (only the "admin" account can remotely login). Use an SSH client such as PuTTY to connect. Make sure the specified ports have been opened on the router or firewall.



To use SFTP (SSH File Transfer Protocol/Secure File Transfer Protocol), make sure the option "Allow SSH connection" has been enabled.

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.



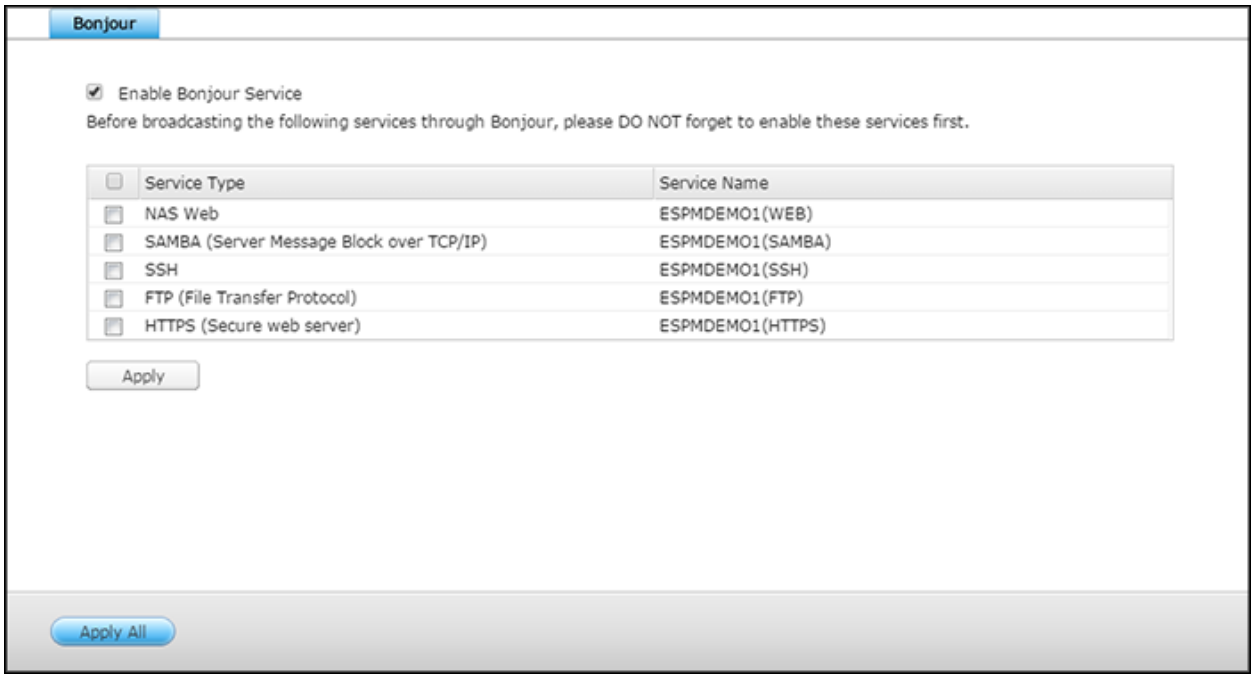
The fields are described as below:

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.
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 user name, authentication protocol/password, and privacy protocol/password.
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.

	Note: MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. You have to assign the correct OID to retrieve the NAS info. The default OID for enterprise NAS is .1.3.6.1.4.1.24861.2

Service Discovery

Go to "Control Panel" > "Network Services" > "Service Discovery" to configure Bonjour.



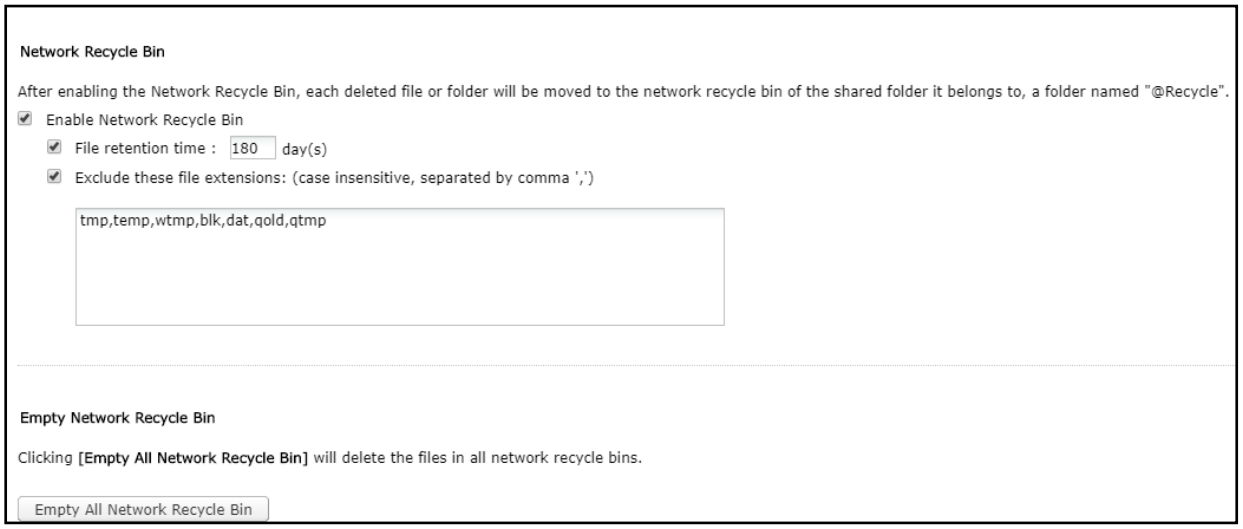
Bonjour

Bonjour provides a general method for macOS to discover services on the local network. By enabling 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.

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.
You can specify the number of days (1-180) to retain files and the file extensions to be excluded from the bin. This feature only supports file deletion via Samba, FTP and File Station.



Using the Network Recycle Bin

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

In File Station:

- 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 "Delete".
- To empty the recycle bin for an individual shared folder, right click inside the recycle bin and select "Empty Recycle Bin".

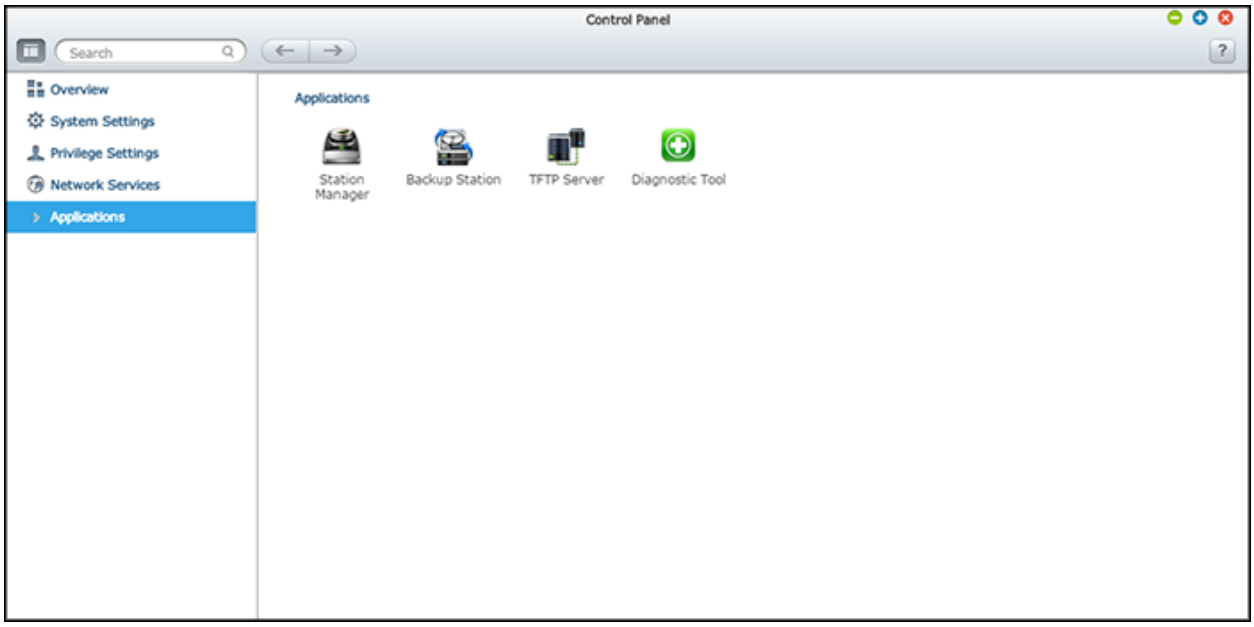
Restricting access to Network Recycle Bin

The Network Recycle Bin can be restricted to administrators usage by going to "Control Panel" > "Storage Manager" > "Shared Folders". Select a shared folder, click "Actions" > "Edit Properties", click "Edit" in "Advanced Settings", enable Network Recycle Bin 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".

Applications

The following NAS functions are designed to meet business needs.

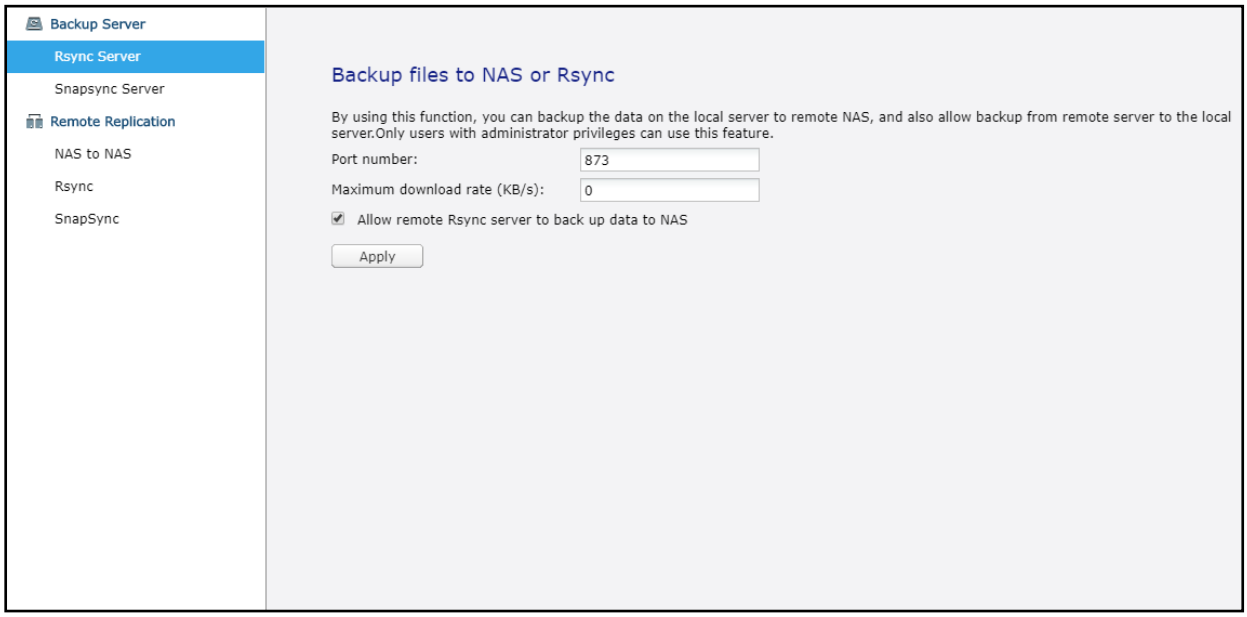


For setup details, refer to the following links:

- Backup Station
- Diagnostic Tool
- File Station
- Station Manager
- TFTP Server
- Virtualization

Backup Station

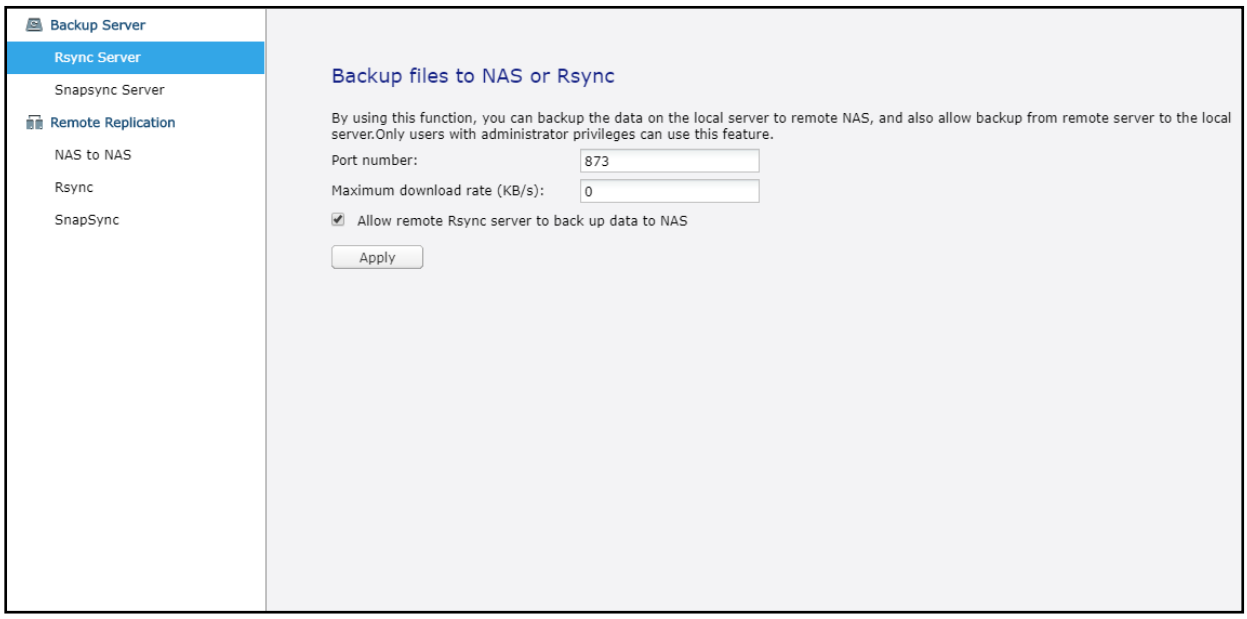
Configure the NAS as a backup server or remote replication with Backup Station.



For details on the features, please refer to the following links:

- Backup Server
- Remote Replication

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.

- **Allow remote Rsync server to back up data to the NAS:** Select this option to allow data backup from a remote Rsync server or NAS server to the local NAS.

Note:

- You can create a maximum of 256 Rsync jobs on the NAS.
- Currently, sending files from Linux to QES requires Rsync via SSH.

SnapSync Server

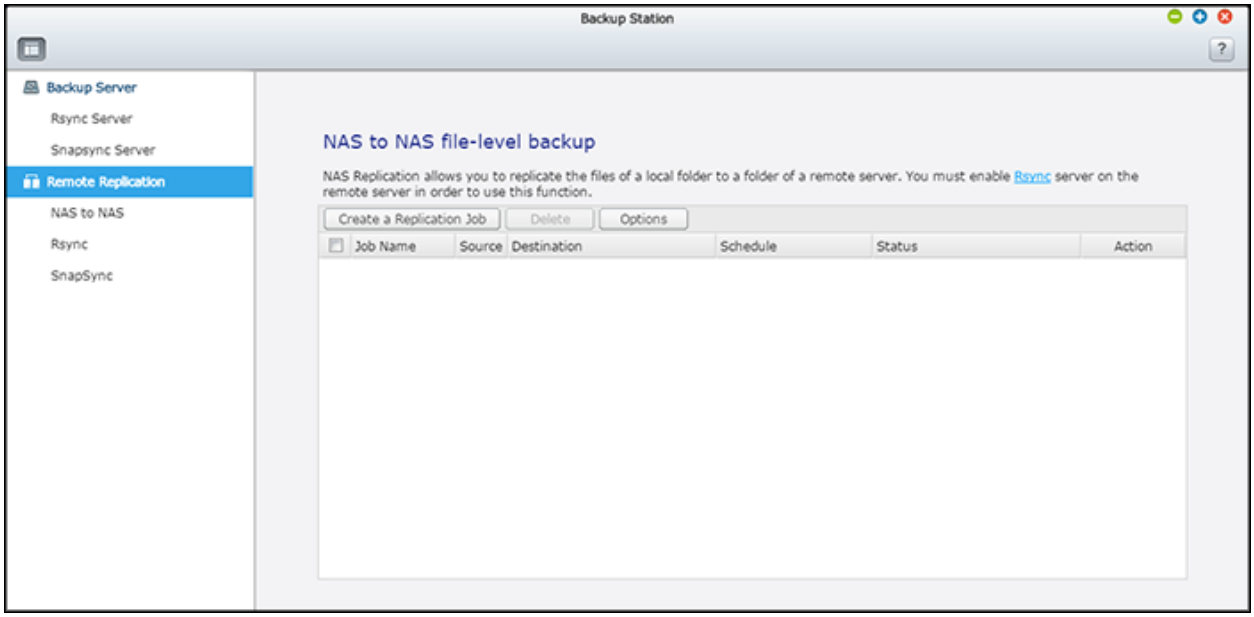
SnapSync server allows a remote NAS to replicate data by snapshot replication to the local NAS. You have to enable SnapSync server before allowing remote NAS to connect, you can also configure service network port, maximum download rate, and the list of trusted remote hosts that are allowed to connect the SnapSync server.

For the remote host list, you can:

- Click "Create Host" and enter the IP address, port, username and password of the remote host and click "Apply". The remote host is added to the list
- Select a host from the list and click "Delete" to remove that host. All SnapSync jobs using the host must be removed first.
- Select a host from the list and click "Test" to verify the connection setting of that host.

Note: Only the "admin" user or a user in the “Administrators” group can create a host.

Remote Replication



This chapter covers the following topics:

- NAS to NAS and Rsync
- SnapSync
- Deleting Replication Jobs

NAS to NAS and Rsync

Source	Destination	Method
QES	QES or QTS	NAS to NAS
QES	Linux	Rsync
QTS	QES	NAS to NAS
Linux	QES	Rsync (with SSH)

The NAS data can be backed up to a remote NAS or Rsync server using Rsync remote replication. Pre-requisite: If the backup destination is a QES NAS, then on the destination NAS go to "Control Panel" > "Applications" > "Backup Station" > "Rsync Server" and enable "Allow remote Rsync server to back up data to the NAS".

For both NAS to NAS and Rsync, to create a replication job:

1. Go to "Control Panel" > "Applications" > "Backup Station" > "Remote Replication".
2. Select either "NAS to NAS" or "Rsync" in the left side panel.
3. Click "Create a Replication Job".
4. Specify a job name.

5. Click "Settings" and 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.
6. (Optional) Enable encryption. SSH connections must be enabled on the remote host, the port number must be the same as the SSH port of the remote host, and the username must have permissions to perform SSH encrypted backup jobs.
7. Click "Test" to verify the connection, then click "Apply".
8. Specify the local folder by clicking the Source folder box. After expanding and locating the folder, click on it to set it as the directory where the data will be replicated from.
9. Specify the destination folder in the Destination folder box. Locate the folder in the folder tree and click on it to set it as the directory where the data will be replicated to. Then click "Add".
10. Click "Backup frequency" to configure the backup schedule.
11. Specify the following options for remote replication jobs by clicking "Options":
    - Activate file compression: Allows file compression during the data transfer process. This option is recommended for low bandwidth environments or remote replication over WAN.
    - Perform incremental replication: When this option is enabled, after the first-time replication, the NAS will only back up files that have been changed since the last backup. The files of the same name, size, and modified time will not be copied again. Enabling this option is recommended for replication jobs to shorten the backup time.
    - Delete extra files on remote destination: Select this option to synchronize the source data with the destination data (one-way synchronization). Extra files on the destination will be deleted. Source data will remain unchanged.
    - Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turning on this option may reduce the time required for remote replication.
    - Replicate ACL and extended attributes: Select this option to replicate ACL and extended attributes.
12. Send alert emails when the following events occur: Receive an email alert each time a job fails or finishes successfully. The SMTP server must be configured at "Control Panel" > "System Settings" > "Notification" > "SMTP Server".
13. Click "Apply". If you select "Execute backup immediately", the replication task will start at once. Otherwise it will run according to the schedule. Note that the job is recursive. Do not turn off the local NAS and the remote server when remote replication is running.

Refer to the following table for button descriptions:

Icon	Name	Description
	Start	Start a replication job immediately.
	Stop	Stop a running replication job.

	Rsync Log	View Rsync logs (replication results).
	Edit	Edit a replication job.
	Disable	Disable replication schedule.
	Enable schedule	Enable replication schedule. Enabled only when a schedule has been created.

To configure the timeout and retry settings of the replication 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 after 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.

SnapSync

You can replicate snapshots to a remote QES NAS using SnapSync.
Pre-requisite: On the destination NAS, go to "Control Panel" > "Applications" > "Backup Station" > "Backup Server" > "SnapSync Server" and select “Enable SnapSync Server”.

To create a replication job on the source NAS:

1. Go to "Control Panel" > "Applications" > "Backup Station" > "Remote Replication" > "SnapSync".
2. Click "Create a Replication Job".
3. Enter a job name and choose whether to replicate to a local interface or remote host. If you select “remote host”, select the host from the dropdown list, or click "Add" to add a host.
4. Choose the source pool (or all drives) from the dropdown list and the shared folder/LUN in the Source Pool box.
5. Click "New" button to enter a drive name for SnapSync. If a SnapSync LUN/shared folder has been used before, it will appear in the dropdown list and you can reuse it for replication.
6. Click "Backup frequency" to specify a backup schedule.
7. Specify the following options for remote replication jobs by clicking "Options" and click "Apply".
   - Compression: Allows file compression during the data transfer process. This option is recommended for low bandwidth environments or remote replication over WAN.

- Deduplication: This option, once checked, allows the system to reduce the amount of bandwidth needed by eliminating duplicate copies of repeating data.
- Send alert emails when the following events occur: Receive an email alert each time a job fails or finishes successfully. The SMTP server must be configured at "Control Panel" > "System Settings" > "Notification" > "SMTP Server".

8. Click "OK". If you select "Execute backup immediately", the replication task will start at once. Otherwise it will run according to the schedule. Note that the job is recursive. Do not turn off the local NAS and the remote server when remote replication is running.

To manage a job, refer to the following table for available actions:

Icon	Name	Description
	Start	Start a replication job immediately.
	Stop	Stop a running replication job.
	Edit	Edit a replication job.
	Suspend job	Suspend SnapSync job.
	Resume job	Resume SnapSync job. State will be "local-updated".

Deleting Replication Jobs

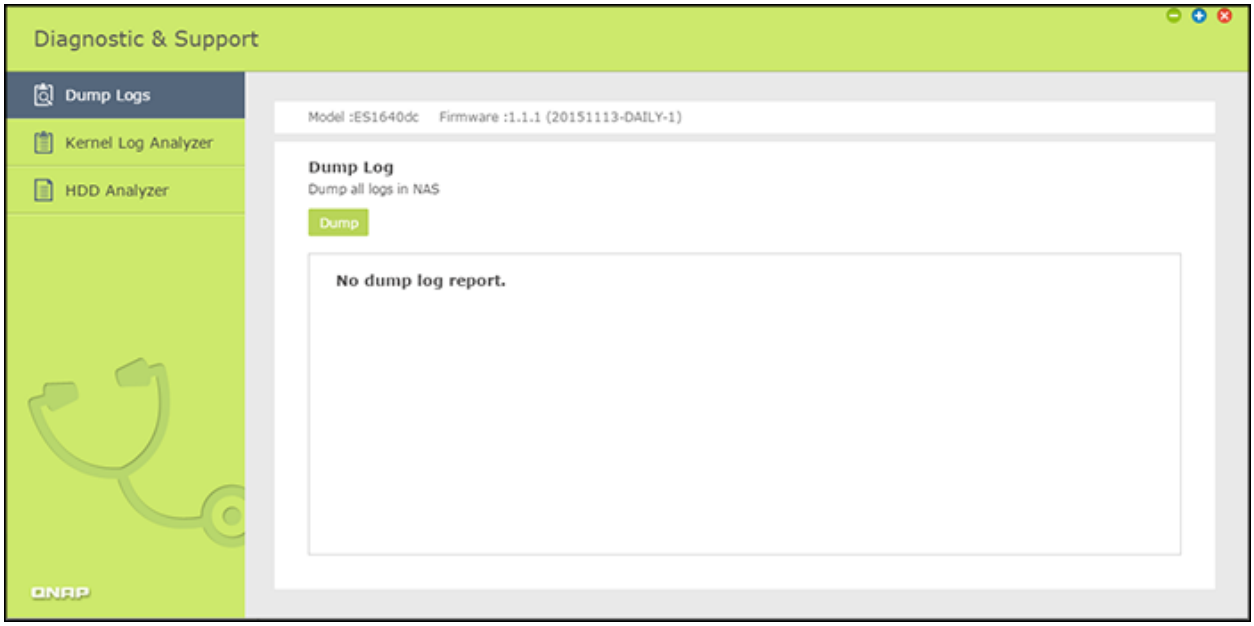
1. Select a replication job from the list.
2. Click "Suspend job", then click "Delete".
3. Click "OK".

Note:

- SnapSync is only available for NAS running QES.
- The replicated LUN snapshots will be listed as un-mapped LUNs in "Storage Manager" > "iSCSI Storage".
- To access the remote replication folder, you need to enable a CIFS, NFS or FTP on the destination NAS and then configure permissions.
- When a replication job is running, the remote replication folder is read-only. If replicating to an iSCSI LUN, the LUN cannot be discovered or accessed.
- When a replication job is suspended, data in the remote replication folder can be modified. If replicating to an iSCSI LUN, the LUN can be discovered and mounted with read/write access.

Diagnostic Tool

The Diagnostic Tool provides a variety of system analysis functions to check the stability of the QNAP NAS. Users can export system kernel records to quickly check if abnormal operations have recently occurred, or they can send the records to QNAP's technical support staff for further investigation. There are also tools for checking the file system, hard drives and RAM.



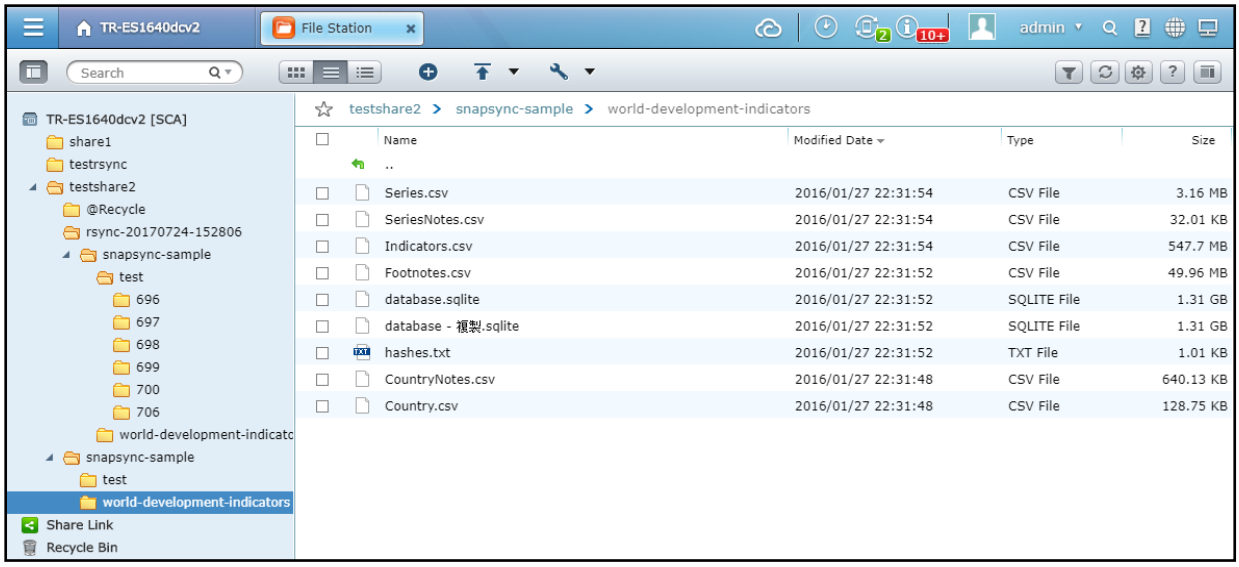
Note: The Diagnostic Tool aims to efficiently troubleshoot NAS issues and is strongly recommended to be used under guidance from QNAP's technical support staff.

With the Diagnostic Tool, you can:

- Dump system logs: Click "Dump Logs" > "Dump" and the system will produce a zip file. Download the zip file and send it to QNAP's technical support staff for further investigation.
- Analyze kernel logs: Click "Kernel Log Analyzer" > "Start" and the result will be shown in the page.
- Analyze HDDs: Click "HDD Analyzer" and choose to dump S.M.A.R.T test logs, perform system performance tests or dump RAID logs. You should send these logs to QNAP's technical support staff when you open a technical support request.

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, set file and folder permissions, and easily share your files and folders on the NAS.



Topics covered in this chapter:

- Starting File Station
- The File Station Interface
  - Menu bar
  - Left panel
  - Right panel
- Using File Station
  - Creating shared folders
  - Subfolder operations
  - File operations
  - Finding your files/folders quickly
  - Setting file/folder level permission
  - Sharing files

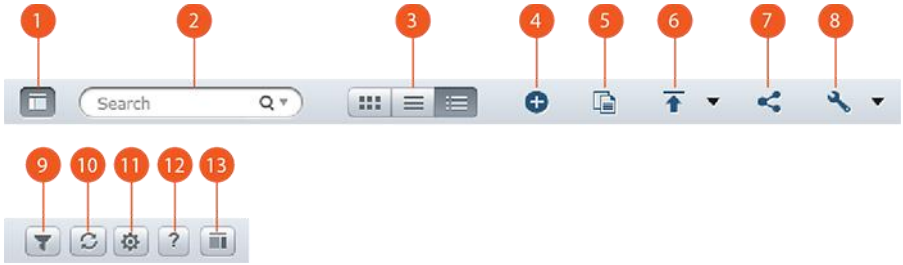
Starting File Station

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.

For dual controller NAS models, use the management interface IP address.

The File Station Interface

Menu bar



No.	Name	Description
1	Left Panel	Hide/Show the left panel.
2	Search Bar	Search files by their name, file type (music, video, or photo) or with advanced search.
3	Browsing Mode	Switch between different browsing modes. From left to right: • Show items as icons • Show items in a list • Show items in a detail list
4	Create folder	Create a folder.
5	Copy/Paste	Copy/paste selected folders or/and files.
6	Upload	Upload files or folders to the selected shared folder or subfolder.
7	Share	Share the folder/file via email or create a shared link. For details, see Sharing files.
8	More Action	• Add to Favorites (and it will appear under "Favorites" on the left panel). • Perform file or folder operations including open, download, rename, move, delete, cut and compress. • Check folder properties. • Review background tasks (file compression, file upload and moving files within the NAS).
9	Smart File Filter	Filter files based on conditions set by users and the conditions will apply to all folders.
10	Refresh	Refresh the current page.

11	Settings	• Set to show/hide files and folders on the local PC (The Java JRE must be installed to use this feature). • Set to show/hide hidden files. • Allow all users to create shared links (for administrators only).
12	Help	Review the online help.
13	Right Panel	Show/Hide the right panel.

Tip: You can drag & drop files from your PC to File Station.

Left panel

- NAS Server: Every shared folder and subfolder on the NAS is listed here.
- Favorites: Bookmarked folders are listed here.
- Local folders: Folders on your local PC are listed here. The Java JRE must be installed to use this feature.
- Share Link: Links of files shared from the NAS are listed here.
- Recycle Bin: Deleted files or folders can be found here.

Right panel

- Properties: Click this tab to review file and folder details. You can also click "Calculate Size" to calculate the total size of all data in the selected folders.
- Permission: Click this tab to configure shared folder permissions. For steps on setting folder permissions, please refer to the below "Setting file/folder level permission" section.

Using File Station

Subfolder operations

Right click on a subfolder and choose to perform 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; • Set sharing details

Open	Enter the chosen subfolder.
Download	Compress and download the subfolder.
Rename	Rename the subfolder.
Move	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 Favorites	Bookmark the subfolder and it will appear under "Favorites" in the left panel.
Compress(Zip)	Compress the subfolder.
Properties	Switch to open the right panel.

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 on a file and choose to perform 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 to another shared folder.
Share	Share selected files/folders via email, by shared links, or to other NAS users. Refer to the Sharing files section for more details.
Open	Open the file with a corresponding application on your PC. If such applications are not available, the file will be downloaded instead.
Download	Download the file. If multiple files are selected for download, they will be

	compressed before the download.
Rename	Rename the file.
Move	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.
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	Switch to open the right panel.

Note:

- Due to limitations with Google Chrome, after clicking “upload” in the File toolbar, only folders that contain at least one file can be uploaded. You can use drag & drop to work around this limitation.
- For Google Chrome, multiple files and folders can be dragged & dropped into File Station to upload them directly.

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 on the magnifier in the search bar and then "Advanced Search". Specify the search conditions (including name, size, modified date, 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 on "Smart File Filter" in the Main Menu. Specify the filtering conditions (including name, size, modified date, 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.

Note: To search all folders on the NAS using advanced search, click the drop down list in "Location" and select "...".

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, select "Properties" and click on the "Permission" on the right panel. 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.

Note:

You can set advanced folder permissions for individual users and user groups:

1. Go to "Control Panel" > "Storage Manager" > "Storage Space" > "Storage Pool List"
2. Select a storage pool.
3. Select a shared folder.
4. Click "Permissions".

You can now set different permission types for a shared folder (NFS host access, user and group permission, and Microsoft Networking host access). Please refer to the Shared Folder chapter for details.

Sharing files

To share files on the NAS using File Station, right click on the files/folders and select "Share". You can configure the settings for sharing files/folders:

- Send (sharing via email): Enter the required fields (including recipient, subject, message, and mail server from NAS or local computer). Click "Send" to share the files via email.
- Settings: Specify the link name, domain name/IP, whether to include SSL (https://) in the URL, and optionally set an expiration time and password for accessing shared files.

Note:

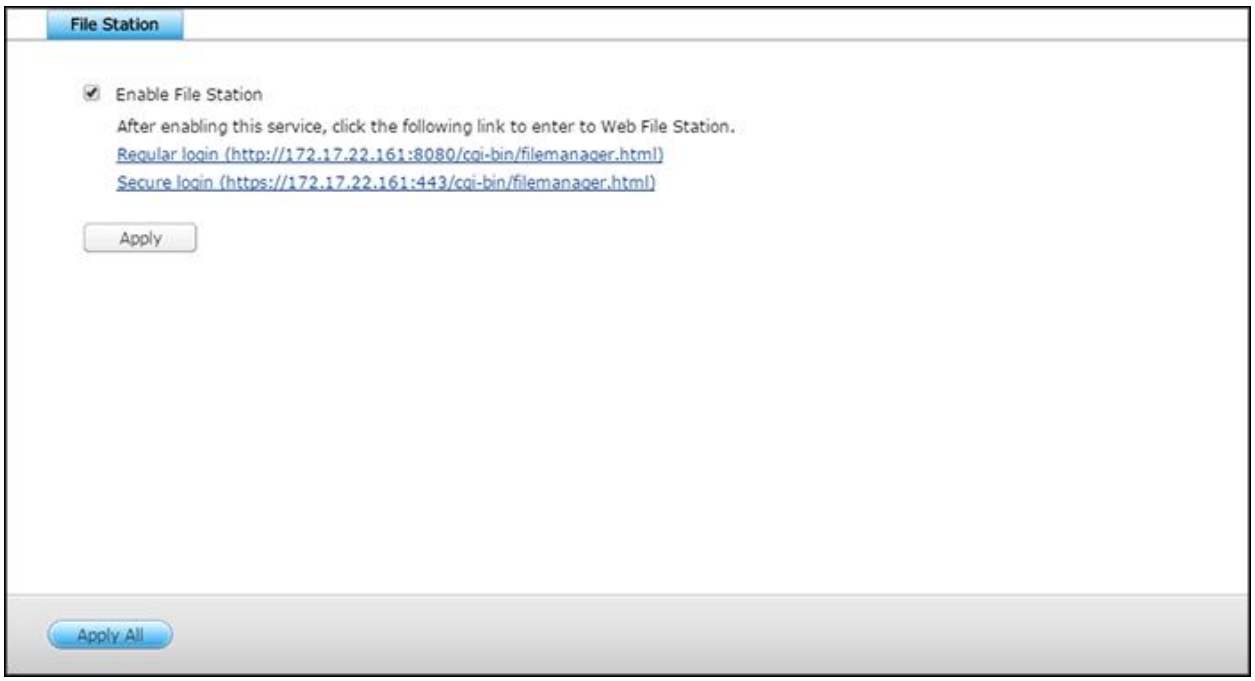
- To share links by email, the email server settings must be properly configured in “Control Panel” > "System Settings" > "Notification" > "SMTP Server".
- Up to 1000 sharing links are supported.
- For best performance, use the latest version of one of the following browsers: Internet Explorer, Firefox, Safari, Chrome.
- Do not close the browser before the file transfer process (upload or download) is completed or the process will fail.
- When transferring a large amount of files over CIFS/SMB using a remote connection, 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.

Station Manager

The Station Manager is an integrated control panel for all QNAP Stations and they can be enabled or disabled here. Currently the only station on QES is File Station.

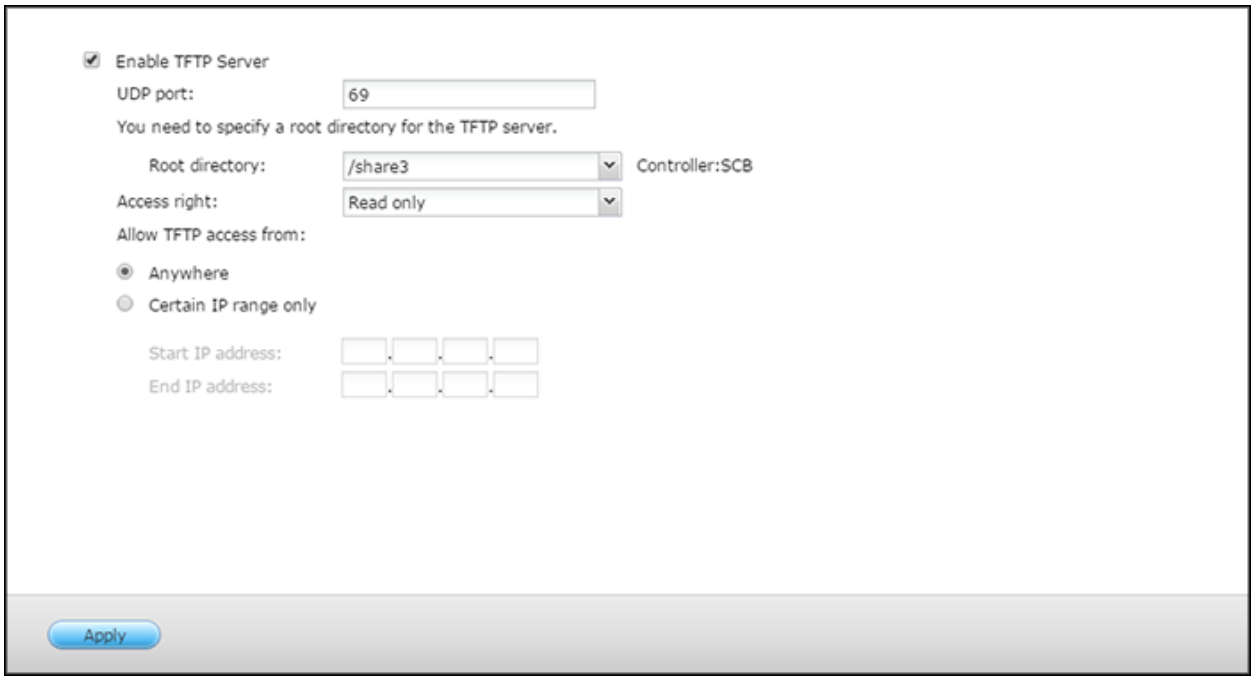


Enabling File Station

Check "Enable File Station" and click the below links to directly login into the application. File Station can only be launched after it is enabled in the Station Manager. For more File Station details please refer to the File Station chapter.

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:

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. Assign read only or full access to the clients.
5. Restrict the TFTP client access by specifying the IP address range or select "Anywhere" to allow any TFTP client access.
6. Click "Apply".

Virtualization

QNAP ES 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 transmission speeds and the SSD Cache feature that capitalizes on SSD technologies. Besides, the remarkable QNAP vSphere Client and QNAP SMI-S Provider are available to increase management productivity and efficiency.

Topics covered in this chapter:

VAAI for iSCSI and VAAI for NAS

For details on VAAI for iSCSI and VAAI for NAS, check here.

ODX (Offloaded Data Transfer)

The ES 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 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.

10 GbE Support

A 10GbE (10 Gigabit Ethernet) 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 ES NAS series is an affordable and reliable storage solution for deploying a 10GbE environment. For detail on 10Gbe 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 ES 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 ES NAS, check here.

vSphere Client

The vSphere Client for QNAP ES NAS is an interface between ESXi and the ES NAS. This tool allows system administrators to manage VMware datastores on the QNAP ES NAS directly from the vSphere Client console and verify the status of all QNAP ES 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). With this tool, the 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.

BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

CDDL License

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE Version 1.0 (CDDL-1.0)

1. Definitions.

1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.

1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

1.4. Executable means the Covered Software in any form other than Source Code.

1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.

1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

1.7. License means this document.

1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. Modifications means the Source Code and Executable form of any of the following:

A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

B. Any new file that contains any part of the Original Software or previous Modification; or

C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.12. Source Code means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, You includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. The Initial Developer Grant: Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant: Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.
(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code: Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications: The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices: You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms: You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions: You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.6. Larger Works: You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions: Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions: You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions: When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN AS IS BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTYS NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) and commercial computer software documentation as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble

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

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

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

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

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

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

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

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of

protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

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

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

TERMS AND CONDITIONS

0. Definitions.
'This License' refers to version 3 of the GNU General Public License.

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

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

To 'modify' a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a 'modified version' of the earlier work or a work 'based on' the earlier work.

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

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

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

An interactive user interface displays 'Appropriate Legal Notices' to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided),

that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

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

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

The 'System Libraries' of an executable work include anything, other than the work as a whole, that:

a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and
b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A 'Major Component', in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

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

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

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

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

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

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

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

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

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

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

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

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to 'keep intact all notices'.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an 'aggregate' if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

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

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to

find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

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

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

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

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

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

7. Additional Terms.

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

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

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

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered 'further restrictions' within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

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

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

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

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

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

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

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

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

An 'entity transaction' is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

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

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

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

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

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

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. 'Knowingly relying' means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your

recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

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

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

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

12. No Surrender of Others' Freedom.
If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

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

14. Revised Versions of this License.

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

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

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

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

15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

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

17. Interpretation of Sections 15 and 16.
If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an

absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS