



QTS 4.3.5/4.4

User Guide

Contents

1. Preface

Audience.....	7
Document Conventions.....	7

2. Overview

NAS Access.....	8
Accessing the NAS Using a Browser.....	8
Accessing the NAS Using Qfinder Pro.....	9
Accessing the NAS Using Qmanager.....	9
2-step Verification.....	10
About QTS.....	11
QTS Navigation.....	12
Task Bar.....	12
Main Menu.....	20
Desktop.....	22
Getting Started.....	26

3. Storage & Snapshots

QTS Flexible Volume Architecture.....	27
Global Settings.....	28
Storage Global Settings.....	28
Disk Health Global Settings.....	29
Snapshot Global Settings.....	30
Storage.....	31
Disks.....	31
Volumes.....	36
Storage Pools.....	50
RAID.....	56
Qtier.....	64
Qtier Benefits.....	64
Qtier Requirements.....	66
Qtier Creation.....	67
Qtier Management.....	70
Tiering On Demand.....	73
Snapshots.....	73
Snapshot Storage Limitations.....	74
Snapshot Creation.....	74
Snapshot Management.....	75
Snapshot Data Recovery.....	76
Snapshot Clone.....	79
Snapshot Replica.....	80

4. System Settings

General Settings.....	91
Configuring System Administration Settings.....	91
Configuring Time Settings.....	92
Configuring Daylight Saving Time.....	93
Configuring Codepage Settings.....	93
Configuring Region Settings.....	94
Configuring the Login Screen.....	94
Security.....	94

Configuring the Allow/Deny List.....	94
Configuring Network Access Protection.....	95
Certificate & Private Key.....	96
Configuring the Password Policy.....	97
Hardware.....	98
Configuring General Hardware Settings.....	98
Configuring Audio Alert Settings.....	99
Configuring Smart Fan Settings.....	99
Backup Battery Unit (BBU).....	100
Configuring Graphics Card Settings.....	100
Power.....	101
EuP Mode.....	101
Wake-on-LAN (WOL).....	101
Power Recovery.....	102
Power Schedule.....	102
Firmware Update.....	103
Checking for Live Updates.....	103
Updating the Firmware Manually.....	103
Updating the Firmware Using Qfinder Pro.....	104
Backup/Restore.....	105
Backing Up System Settings.....	105
Restoring System Settings.....	105
System Reset and Restore to Factory Default.....	105
External Device.....	107
USB Printer.....	107
Uninterruptible Power Supply (UPS).....	108
System Status.....	110
System Logs.....	111
System Event Logs.....	111
System Connection Logs.....	111
Online Users.....	112
Syslog Client Management.....	113
Resource Monitor.....	113

5. Privilege

Users.....	115
Default User Accounts.....	115
Creating a Local User.....	115
Creating Multiple Users.....	116
User Account Lists.....	118
Importing Users.....	119
Exporting Users.....	120
Modifying User Account Information.....	120
Deleting Users.....	121
Home Folders.....	122
User Groups.....	122
Default User Groups.....	122
Creating a User Group.....	122
Modifying User Group Information.....	123
Deleting User Groups.....	124
Shared Folders.....	124
Default Shared Folders.....	124
Creating a Shared Folder.....	125
Editing Shared Folder Properties.....	127
Refreshing a Shared Folder.....	128
Removing Shared Folders.....	128
Snapshot Shared Folders.....	129

ISO Shared Folders.....	131
Shared Folder Permissions.....	133
Shared Folder Access.....	136
Folder Aggregation.....	141
Shared Folder Encryption.....	144
Quota.....	146
Configuring Quota Settings.....	147
Editing Quota Settings.....	147
Exporting Quota Settings.....	147
Domain Security.....	147
Active Directory (AD) Authentication.....	148
LDAP Authentication.....	150
AD and LDAP Management.....	152
Domain Controller.....	153
Enabling a Domain Controller.....	154
Resetting a Domain Controller.....	155
Default Domain User Accounts.....	155
Creating a Domain User.....	155
Creating Multiple Domain Users.....	156
Domain User Account Lists.....	157
Modifying Domain User Account Information.....	159
Deleting Domain Users.....	160
Domain User Groups.....	160
Computers.....	162
DNS.....	163
Back Up/Restore.....	166

6. Network & Virtual Switch

About Network & Virtual Switch.....	168
Basic and Advanced Mode.....	168
Overview.....	168
Interfaces.....	169
IP Address.....	169
DNS.....	171
Virtual LANs (VLANs).....	172
Port Trunking.....	173
System Default Gateway.....	174
USB QuickAccess.....	174
Wi-Fi.....	176
Thunderbolt.....	179
Virtual Switches.....	181
Creating a Virtual Switch in Basic Mode.....	182
Creating a Virtual Switch in Advanced Mode.....	182
Creating a Virtual Switch in Software-defined Switch Mode.....	185
DHCP Server	186
Creating a DHCP Server	187
RADVD.....	189
Route.....	192
Creating a Static Route.....	193
DDNS.....	194
Adding a DDNS Service.....	194

7. Network & File Services

Network Access.....	195
Service Binding.....	195
Proxy.....	195

Win/Mac/NFS.....	196
Microsoft Networking.....	196
Apple Networking.....	198
NFS Service.....	198
Telnet/SSH.....	199
Configuring Telnet Connections.....	199
Configuring SSH Connections.....	199
Editing SSH Access Permissions.....	199
SNMP.....	200
Configuring SNMP Settings.....	200
SNMP Management Information Base (MIB).....	201
Service Discovery.....	202
UPnP Discovery Service.....	202
Bonjour.....	202
Network Recycle Bin.....	202
Configuring the Network Recycle Bin.....	202
Deleting All Files in the Network Recycle Bin.....	203
Restricting Access to the Network Recycle Bin.....	203

8. File Station

Overview.....	204
About File Station.....	204
System Requirements.....	204
Supported File Formats.....	204
Parts of the User Interface.....	205
Settings.....	207
File Operations.....	209
Uploading a File.....	210
Downloading a File.....	211
Opening a File.....	211
Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension.....	212
Opening a Text File Using Text Editor.....	212
Viewing a File in Google Docs.....	213
Viewing a File in Microsoft Office Online.....	213
Viewing File Properties.....	213
Modifying File Permissions.....	214
Sorting Files.....	215
Copying a File.....	215
Moving a File.....	216
Renaming a File.....	217
Deleting a File.....	218
Restoring a Deleted File.....	218
Mounting an ISO File.....	219
Unmounting an ISO File.....	219
Compressing a File.....	219
Extracting Compressed Files or Folders.....	220
Sharing a File or Folder by Email.....	221
Sharing a File or Folder on a Social Network.....	222
Sharing a File or Folder Using Share Links.....	223
Sharing a File or Folder with a NAS User.....	224
Playing an Audio File.....	225
Playing a Video File.....	226
Opening Image Files Using Image2PDF.....	226
Opening a 360-degree Image or Video File.....	226
Streaming to the Network Media Player.....	227
Adding a File to the Transcode Folder.....	228
Canceling or Deleting Transcoding.....	228

Viewing Transcode Information.....	229
Folder Operations.....	229
Uploading a Folder.....	230
Uploading a Folder Using Drag and Drop.....	231
Viewing and Modifying Folder Properties.....	231
Viewing Storage Information.....	233
Modifying Folder Permissions.....	233
Viewing Qsync Folders.....	234
Managing Share Links.....	235
Viewing Files and Folders Shared with Me.....	235
Creating a Folder.....	235
Copying a Folder.....	236
Creating a Desktop Shortcut.....	236
Adding a Folder to Favorites.....	237
Removing a Folder from Favorites.....	237
Compressing a Folder.....	238
Deleting a Folder.....	238
Creating a Shared Folder.....	239
Creating a Snapshot Shared Folder.....	241
Sharing Space with a New User.....	242
Adding a Folder to the Transcode Folder.....	243
Canceling or Deleting Transcoding.....	244
Remote Mount.....	244
About Remote Mount.....	244
Remote Mount Limitations.....	245
Creating Remote Mount.....	245
Viewing Recent Connection Records.....	247
Viewing Current Connection Status.....	247

9. License Center

Buying Licenses Using QNAP ID.....	248
License Activation.....	249
Activating a License Using QNAP ID.....	249
Activating a License Using a Product or License Key.....	250
Activating a License Using a PAK.....	251
Activating a License Offline.....	251
License Deactivation.....	253
Deactivating a License Using QNAP ID.....	253
Deactivating a License Offline.....	253
License Extension.....	254
Extending a License Using QNAP ID.....	255
Extending a License Offline Using an Unused License.....	255
Extending a License Offline Using a Product Key.....	257
Extending a License by Purchasing Online.....	258
License Management.....	259
Recovering Licenses.....	259
Transferring a License to the New QNAP License Server.....	259
Deleting a License.....	260

10. Notification Center

Overview.....	261
Notification Queue and History.....	261
Queue.....	261
History.....	261
Service Account and Device Pairing.....	262
Email Notifications.....	263

SMS Notifications.....	264
Instant Messaging Notifications.....	266
Push Notifications.....	268
System Notification Rules.....	270
Event Notifications.....	270
Alert Notifications.....	274
Global Notification Settings.....	277
System Logs.....	278

11. SSD Profiling Tool

SSD Over-Provisioning.....	279
SSD Extra Over-Provisioning.....	279
SSD Over-Provisioning Tests.....	279
Creating an SSD Over-Provisioning Test.....	279
Review.....	280
Test Reports.....	281
Test Report Actions.....	281
Test Report Information.....	282
Settings.....	282

1. Preface

Audience

This document is intended for consumers and storage administrators. This guide assumes that the user has a basic understanding of storage and backup concepts.

Document Conventions

Symbol	Description
	Notes provide default configuration settings and other supplementary information.
	Important notes provide information on required configuration settings and other critical information.
	Tips provide recommendations or alternative methods of performing tasks or configuring settings.
	Warnings provide information that, when ignored, may result in potential loss, injury, or even death.

2. Overview

NAS Access

Method	Description	Requirements
Web browser	You can access the NAS using any computer on the same network if you have the following information: - NAS name (Example: http://example123/) or IP address - Logon credentials of a valid user account For details, see Accessing the NAS Using a Browser.	- Computer that is connected to the same network as the NAS - Web browser
Qfinder Pro	Qfinder Pro is a desktop utility that enables you to locate and access QNAP NAS devices on a specific network. The utility supports Windows, macOS, Linux, and Chrome OS. For details, see Accessing the NAS Using Qfinder Pro.	- Computer that is connected to the same network as the NAS - Web browser - Qfinder Pro
Qmanager	Qmanager is a mobile application that enables administrators to manage and monitor NAS devices on the same network. You can download Qmanager from the Apple App Store and the Google Play Store. For details, see Accessing the NAS Using Qmanager.	- Mobile device that is connected to the same network as the NAS - Qmanager
Explorer (Windows)	You can map a NAS shared folder as a network drive to easily access files using Explorer. For details on mapping shared folders, see Mapping a Shared Folder on a Windows Computer.	- Windows computer that is connected to the same network as the NAS - Qfinder Pro
Finder (macOS)	You can mount a NAS shared folder as a network drive to easily access files using Finder. For details on mounting shared folders, see Mounting a Shared Folder on a Mac Computer.	- Mac computer that is connected to the same network as the NAS - Qfinder Pro

Accessing the NAS Using a Browser

1. Verify that your computer is connected to the same network as the NAS.
2. Open a web browser on your computer.
3. Type the IP address of the NAS in the address bar.

**Tip**

If you do not know the IP address of the NAS, you can locate it using Qfinder Pro. For details, see [Accessing the NAS Using Qfinder Pro](#).

The QTS login screen appears.

4. Specify your username and password.
5. Click **Login**.
The QTS desktop appears.

Accessing the NAS Using Qfinder Pro

1. Install Qfinder Pro on a computer that is connected to the same network as the NAS.

**Tip**

To download Qfinder Pro, go to <https://www.qnap.com/en/utilities>.

2. Open Qfinder Pro.
Qfinder Pro automatically searches for all QNAP NAS devices on the network.
3. Locate the NAS in the list, and then double-click the name or IP address.
The QTS login screen opens in the default web browser.
4. Specify your username and password.
5. Click **Login**.
The QTS desktop appears.

Accessing the NAS Using Qmanager

1. Install Qmanager on an Android or iOS device.

**Tip**

To download Qmanager, go to the Apple App Store or the Google Play Store.

2. Open Qmanager.
3. Tap **Add NAS**.
Qmanager automatically searches for all QNAP NAS devices on the network.
4. Locate the NAS in the list, and then tap the name or IP address.
5. Specify your username and password.
6. Optional: If your mobile device and NAS are not connected to the same subnet, perform one of the following actions.

Action	Steps
Add NAS manually	- Tap Add NAS manually. - Specify the following information. - Host name or IP address of the NAS - Password of the admin account - Tap Save.
Sign in using QID	- Tap Sign in QID. - Specify the following information. - Email address that you used to create your QNAP account - Password of your QNAP account - Tap Sign in. - Locate the NAS in the list, and then tap the name or IP address.

2-step Verification

2-step verification enhances the security of user accounts. When the feature is enabled, users are required to specify a six-digit security code in addition to the account credentials during the login process.

To use 2-step verification, you must install an authenticator application on your mobile device. The application must implement verification services using the Time-based One-time Password Algorithm (TOTP). QTS supports Google Authenticator (for Android, iOS, and BlackBerry) and Authenticator (for Windows Phone).

Enabling 2-step Verification

- Install an authenticator application on your mobile device.
QTS supports the following applications:
 - Google Authenticator: Android, iOS, and BlackBerry
 - Authenticator: Windows Phone
- Verify that the system times of the NAS and mobile device are synchronized.



Tip

QNAP recommends connecting to an NTP server to ensure that your NAS follows the Coordinated Universal Time (UTC) standard.

- In QTS, go to **Options > 2-step Verification**.
- Click **Get Started**.
The **2-step Verification** window opens.
- Open the authenticator application on your mobile phone.
- Configure the application by scanning the QR code or specifying the security key displayed in the **2-step Verification** window.

7. In the **2-step Verification** window, click **Next**.
The **Confirm your 2-step verification settings** screen appears.
8. Specify the security code generated by the authenticator application.
9. Select an alternative verification method that will be used whenever your mobile device is inaccessible.

Method	Steps
Answer a security question.	Select one of the options or provide your own security question.
Email a security code.	a. Go to Control Panel > Notification Center > Service Account and Device Pairing > Email. b. Verify that the SMTP server is correctly configured.

10. Click **Finish**.

Logging in to QTS Using 2-step Verification

1. Specify your username and password.
2. Specify the security code generated by the authenticator application installed on your mobile device.
3. Optional: If your mobile device is inaccessible, click **Verify another way**.
4. Specify the answer to the security question.
5. Click **Login**.

Disabling 2-step Verification

Situation	User Action	Steps
Users are locked out of their accounts.	Administrators can disable 2-step verification from the Control Panel.	1. Go to Control Panel > Privilege > Users. 2. Identify a locked out user, and then click . 3. Deselect 2-step Verification. 4. Click OK.
An administrator is locked out and no other administrators can access the account.	An administrator must restore the factory settings.	Press the RESET button on the back of the NAS for three seconds. The NAS restores the default administrator password and network settings.  Warning Pressing the RESET button for 10 seconds resets all settings and deletes all data on the NAS.

About QTS

QTS is a Linux-based operating system that runs applications for file management, virtualization, surveillance, multimedia, and other purposes. The optimized kernel and various services efficiently manage

system resources, support applications, and protect your data. QTS also has built-in utilities that extend the functionality and improve the performance of the NAS.

The multi-window, multitasking user interface enables you to manage the NAS, user accounts, data, and applications. Out of the box, QTS provides built-in features that allow you to easily store and share files. QTS also links to the App Center, which offers plenty of options for customizing the NAS and improving user workflows.

QTS Navigation

Task Bar



No.	Element	Possible User Actions
1	Show Desktop	Click the button to minimize or restore all open windows.
2	Main Menu	Click the button to open the Main Menu panel on the left side of the desktop.
3	Search	- Type key words to locate settings, applications, and help content. - Click an entry in the search results to open the application, system utility, or Help Center window. If the application is not yet installed, QTS opens the corresponding download screen in the App Center window.
4	Volume Control  Note This feature is only available on models with certain hardware specifications.	Click the button to view the following: - Media Volume: Click and drag the slider thumb to adjust the audio volume for applications that use the built-in speaker or line-out jack. - HD Station - Music Station - OceanKTV - Audio Alert Volume: Click and drag the slider thumb to adjust the volume of system audio alerts.

No.	Element	Possible User Actions
5	Background Tasks	• Position the mouse pointer over the button to see the number of background tasks that are running. Examples of background tasks are file backup and multimedia conversion. • Click the button to see the following details for each background task: • Task name • Task description • Progress (percentage of completion) • Click  to stop a task.
6	External Devices	• Position the mouse pointer over the button to view the number of external storage devices and printers that are connected to the USB and SATA ports on the NAS. • Click the button to view the details for each connected device. • Click a listed device to open File Station and view the contents of the device.
7	Event Notifications	• Position the mouse pointer over the button to see the number of recent errors, warnings, and notices. • Click the button to view the following details for each event: • Event type • Description • Timestamp • Number of instances • Click a list entry to view the related utility or application screen. Clicking a warning or error log entry opens the System Logs window. • Click More>> to open the System Logs window. • Click Clear All to delete all list entries.  Tip You can create notification rules using Notification Center. For details, see System Notification Rules.
8	Options	Click your profile picture to open the Options screen. For details, see Options .

No.	Element	Possible User Actions
9	[USER_NAME]	Click the button to view the last login time and the following menu items: • Options: Opens the Options window For details, see Options. • Sleep: Keeps the NAS powered on but significantly reduces power consumption This feature is only available on models with certain hardware specifications. • Restart: Restarts the NAS • Shutdown: Shuts down QTS and then powers off the NAS  Tip You can also power off the NAS using one of the following methods: • Press and hold the power button for 1.5 seconds. • Open Qfinder Pro, and then go to Tools > Shut down Device . • Open Qmanager, and then go to Menu > System Tools > System . Tap Shutdown. • Logout: Logs the user out of the current session

No.	Element	Possible User Actions
10	More	Click the button to view the following menu items: • Help: Displays links to the Quick Start Guide, Virtualization Guide, Help Center, and online tutorials page • Language: Opens a list of supported languages and allows you to change the language of the operating system • Desktop Preferences: Opens a list of display modes and allows you to select your preferred mode of displaying the QTS desktop based on your device type • Help Request: Opens the Helpdesk window • Data & Privacy: Opens the QNAP Privacy Policy page • About: Displays the following information: • Operating system • Hardware model • Operating system version • Number of installed drives • Number of empty drive bays • System volume name • Used disk space • Available disk space
11	Dashboard	Click the button to display the dashboard. For details, see Dashboard.

Options

Options — ×

< 1 Profile
2 Wallpaper
3 2-step Verification
4 Change Password
5 E-mail Account
6 Misc >



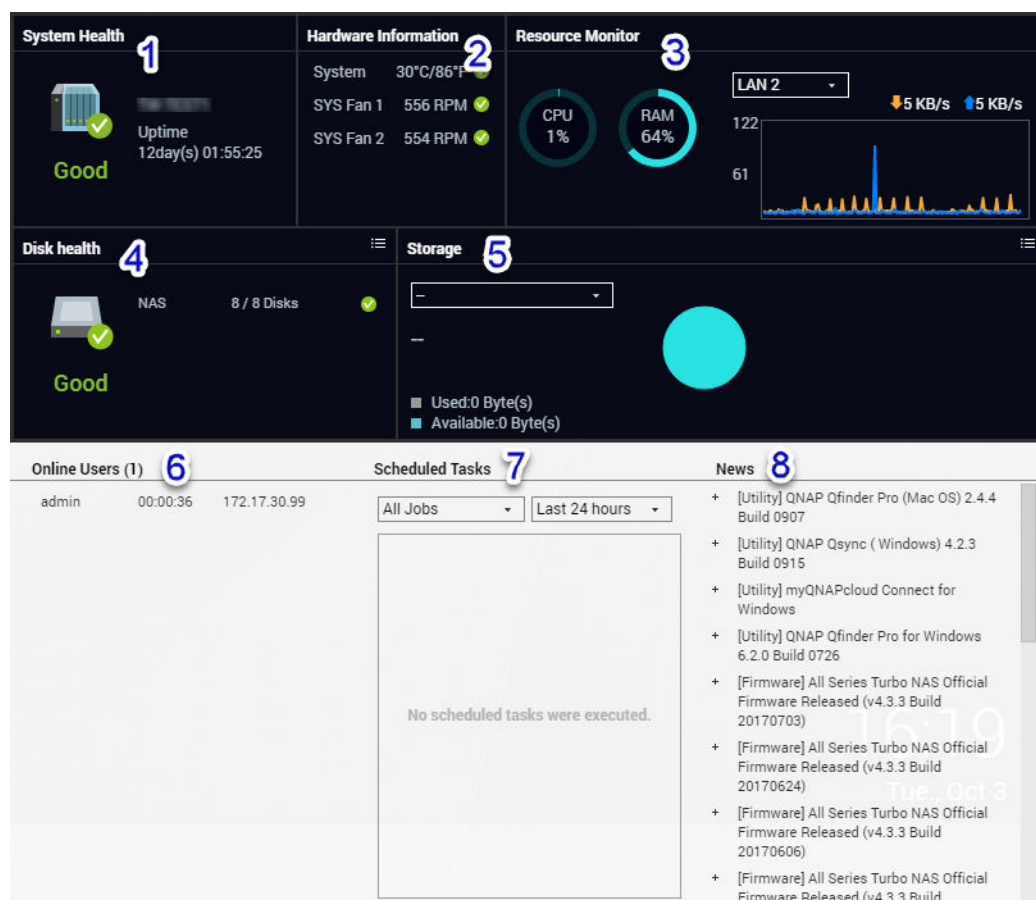
Username: admin
E-mail:
Phone number:

Connection Logs: [View](#)
[Edit login screen](#)

No.	Tab	Possible User Actions
1	Profile	- Specify the following optional information: - Profile picture - Email address - Phone number - Click View to display the System Connection Logs screen. - Click Edit login screen to open the Login Screen configuration screen in the Control Panel window. - Click Apply to save all changes.
2	Wallpaper	- Select a wallpaper from the built-in options or upload a photo. - Click Apply to save all changes.
3	2-step Verification	Click Get Started to open the configuration wizard. For details, see Enabling 2-step Verification .
4	Change Password	- Specify the following information: Old password New password: Specify a password with a maximum of 64 characters. QNAP recommends using passwords with at least 6 characters. - Click Apply to save all changes.
5	E-mail Account	- Add, edit, and delete email accounts that you intend to use to share files. - Click Apply to save all changes.

No.	Tab	Possible User Actions
6	Miscellaneous	• Enable the following settings as necessary. • Auto logout after an idle period: Specify the duration of inactivity after which the user is automatically logged out. • Warn me when leaving QTS: When enabled, QTS prompts users for confirmation whenever they try to leave the desktop (by clicking the Back button or closing the browser). QNAP recommends enabling this setting. • Reopen windows when logging back into NAS: When enabled, the current desktop settings (including all open windows) are retained until the next session. • Show the desktop switching button: When enabled, QTS displays the desktop switching buttons < > on the left and right sides of the desktop. • Show the link bar on the desktop: When enabled, QTS displays the link bar on the bottom of the desktop. • Keep Main Menu open after selection: When enabled, QTS keeps the main menu pinned to the desktop after you open it. • Show a list of actions when external storage devices are detected: When enabled, QTS displays an Autoplay dialog box whenever an external storage device is inserted into a USB or SATA port. • Click Apply to save all changes.

Dashboard



The dashboard opens in the lower right corner of the desktop.



Tip

You can click and drag a section onto any area of the desktop.

No.	Section	Displayed Information	User Actions
1	System Health	- NAS name - Uptime (number of days, hours, minutes and seconds) - Health status	Click the heading to open the System Information screen in the System Status window. If disk-related issues occur, clicking the heading opens the Storage & Snapshots window.
2	Hardware Information	- System temperature - CPU fan speed - System fan speed - System fan speed	Click the heading to open the Hardware Information screen in the System Status window.

No.	Section	Displayed Information	User Actions
3	Resource Monitor	• CPU usage in % • Memory usage in % • Network upload and download speeds/rates	Click the heading to open the Overview screen in the Resource Monitor window.
4	Disk Health	• Number of installed disks • Health status of installed disks	• Click the heading to open the Disk Health screen in the Storage & Snapshots window. • Click  to switch between disk and NAS information. • Click a disk name to view the following information for each installed disk: • Capacity/size • Temperature • Health status • Click Details to open the Overview screen in the Storage & Snapshots window.
5	Storage	For each volume: • Status • Used space • Available space • Folder size For each storage pool: • Status • Used space • Available space • Volume size	• Click the heading to open the Storage Resource screen in the Resource Monitor window. • Click  to switch between volume and storage pool information.
6	Online Users	• User name • Session duration • IP address	Click the heading to open the Online Users screen in the System Logs window.

No.	Section	Displayed Information	User Actions
7	Scheduled Tasks	• Task type • Task summary • Task name • Timestamp • Status	Use the filters to view tasks that were executed within a specific period.
8	News	Links to QNAP announcements	Click the heading to open the relevant pages on the QNAP website.

Main Menu

No.	Section	Description	Possible User Actions
1	NAS Information	Displays the NAS name and model number.	N/A

No.	Section	Description	Possible User Actions
2	System	Displays a list of system utilities and other programs that enable you to manage the NAS. The following are the default system utilities: • Control Panel • Storage & Snapshots • Users • Network & Virtual Switch • myQNAPcloud • Resource Monitor • App Center • Help Center • Qboost • HybridDesk Station  Note This application is only available on models with certain hardware specifications.	• Open a system utility or application in the QTS desktop • Click a menu item. • Right-click a menu item and then select Open. • Open an application in a new browser tab (only for certain apps) • Right-click a menu item and then select Open in new browser tab. • Create a shortcut on the desktop • Right-click a menu item and then select Create shortcut. • Click and drag a menu item to the desktop.
3	Applications	Displays a list of applications developed by QNAP or third-party developers. When an app is installed, it is automatically added to the applications list. The following are the default applications: • Backup Station • File Station • Helpdesk • License Center Notification Center • QTS SSL Certificate	

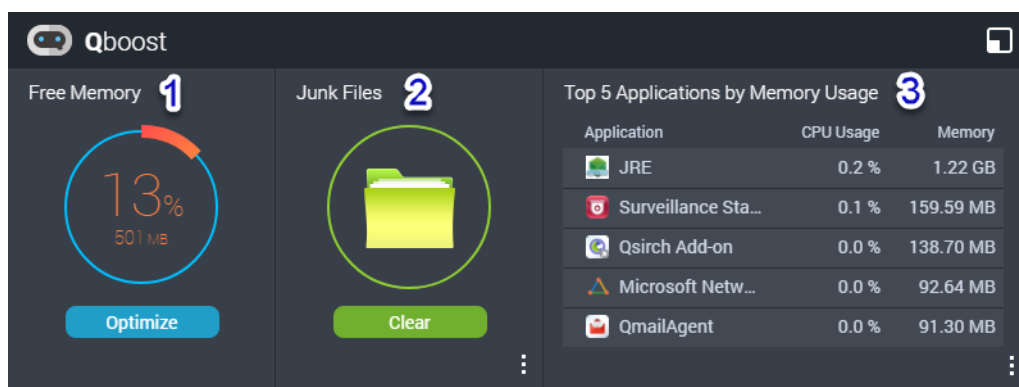
Desktop



#	Element	Description	Possible User Actions
1	Wallpaper	This is a digital image that is used as a background for the QTS desktop. Users can either select from one of the provided wallpapers or upload an image	Change the wallpaper in the Options window.
2	Shortcut icons	This opens an app or a utility. When you install an application, QTS automatically creates a shortcut on the desktop. The following are the default shortcuts: - Control Panel - File Station - Storage & Snapshots - App Center - Help Center	- Click an icon to open the application window. - Right-click an icon and then select one of the following: Open: Opens the application window Remove: Deletes the icon from the desktop - Click and drag an icon to another desktop.
3	Desktop	This area contains open system utilities and applications. The desktop consists of three separate screens.	Click < or > to move to another desktop.
4	Qboost	This enables you to manage and monitor memory consumption.	- Click  or  to display the memory status and open the Qboost panel. - Click  or  to hide the memory status and close the Qboost panel.

#	Element	Description	Possible User Actions
5	Recycle Bin	This displays the list of files that the currently active user moved to the Recycle Bin. The following applications provide users a choice between permanently deleting files and moving files to the Recycle Bin. • File Station • Music Station • Photo Station • Video Station	• Click  to open the Recycle Bin screen in the File Station window. • Right-click  and then select one of the following: • Open: Opens the Recycle Bin screen in the File Station window • Empty All: Permanently deletes files in the Recycle Bin • Settings: Opens the Network Recycle Bin screen in the Control Panel window
6	Date and time	This displays the date and time that the user configured during installation of the operating system.	N/A
7	Link bar	This displays shortcut links to myQNAPcloud, utility and app download pages, feedback channels, and the Helpdesk.	Click any of the following buttons: • : Opens the myQNAPcloud website in another browser tab • : Opens the download page for mobile applications and utilities • : Provides links to the QNAP Wiki, QNAP Forum, and Customer Service portal • : Opens the Helpdesk utility
8	Notifications	This notifies the user about important system events that may or may not require user action. Notifications appear in the lower right corner of the desktop.	Click the notification to open the corresponding utility or app.

Qboost



Qboost is a system utility that monitors and enables you to manage memory consumption. It provides the following information:

#	Section	Description	User Actions
1	Free Memory	- Memory that has not been allocated, is currently unused, and does not contain useful information - Expressed as a percentage of the total memory and the number of bytes	Click Optimize to clear the buffer memory (block level) and cache memory (file level).
2	Junk Files	- Unnecessary system files and files in the Recycle Bin - Consume disk space and memory because they are not automatically deleted when no longer needed	- Click Clear to permanently delete the specified files. By default, clicking Clear only deletes unnecessary system files, such as files that the operating system and applications create while performing certain tasks. - Click  to select other types of files to delete. Select Empty Recycle Bin to include files that were moved to the Recycle Bin by the currently active user.
3	Top 5 Applications by Memory Usage	Top five applications and services that consume the most memory	Click  to display all applications and services that can be enabled and disabled from either the Control Panel or the App Center. For details, see Application Management .

Application Management

Application Management displays the following information.

Item	Description
Application	Displays the application name
CPU Usage	Displays the percentage of consumed processing power
Memory	Displays the amount of memory consumed
CPU Time	Displays the amount of time the CPU requires to process an application request
Status	Displays one of the following statuses: • Always Enabled • Always Disabled • Scheduled
Action	Displays icons for the possible actions

You can perform the following actions.

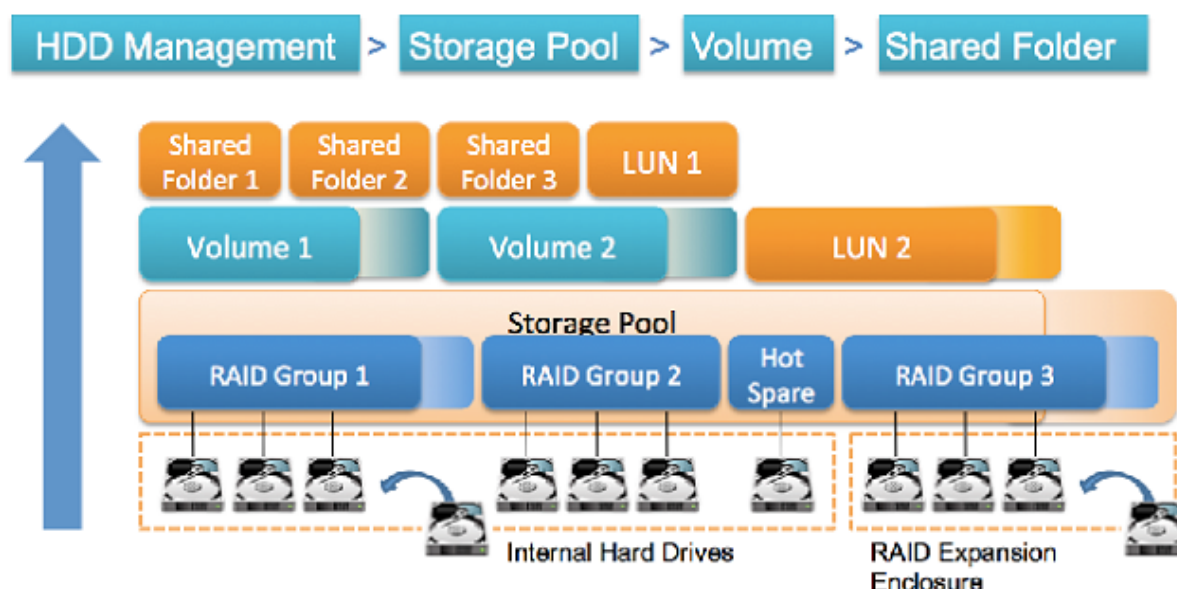
Objective	Action
Enable or disable an application or service.	• Click  to change the status to Always Enabled. • Click  to change the status to Always Disabled.
Create a schedule for enabling and disabling an application or service.  Warning Setting a schedule may force an application to stop in the middle of a task.	1. Click  to open the scheduling screen. 2. Select Enable Schedule. The calendar is activated. All days and hours are enabled by default. 3. Select the hours during which the application or service should be enabled or disabled. Hours are filled with one of the following colors or patterns. • Blue: The application or service is enabled. • Gray: The application or service is disabled. • Striped: The NAS is scheduled to sleep or shut down. 4. Optional: If you want to enable the app at a certain time, specify the number of minutes after the hour when the application is enabled or disabled. Example: To enable an application only after half an hour, type 30. 5. Perform one of the following actions. • Click Apply: Applies the schedule to the selected application or service • Select Auto-apply: Applies the schedule to all applications and services
Delete a schedule.	Click  to delete the schedule and disable an application or service.
Remove an application.	Click  . This function applies only to applications that are available in App Center.

Getting Started

1. Plan how you want to combine or divide the available storage space.
For details, see [Volume Configuration](#).
2. Optional: Create one or more storage pools.
You need to create at least one storage pool to create multiple volumes. For details, see [Creating a Storage Pool](#).
3. Create one or more volumes.
You need to create at least one volume to store files on the NAS. For details, see [Volume Creation](#).
4. Create user accounts.
QNAP recommends creating a user account for each person that requires access to the NAS. For details, see [Creating a Local User](#).
5. Optional: Create user groups.
User groups enable you easily manage user accounts. For details, see [Creating a User Group](#).
6. Optional: Create shared folders.
QTS creates four default shared folders. For details, see [Shared Folders](#).
7. Edit shared folder permissions.
Permissions enable you to control who can view and modify files in a shared folder. For details, see [Shared Folder Permissions](#).
8. Map the shared folders as network drives on your computer.
For details, see [Shared Folder Access](#).
9. Store and manage files.
For details, see [File Station](#).

3. Storage & Snapshots

QTS Flexible Volume Architecture



QTS Flexible Volume Architecture

Object	Description	Details
Disk	A physical device that stores and retrieves data.	QTS restricts which type of disk can be used for SSD cache and storage space (static volumes and storage pools). For details, see Disk Types .
RAID group	A group of one or more disks combined into one logical disk. RAID groups usually contain disks that are of the same type and capacity.	Data is distributed across the disks in a RAID group. Each RAID type offers a different combination of reliability, performance, and capacity. For details, see RAID .
Storage pool	A pool of storage space consisting of one or more RAID groups.	Storage pools can aggregate RAID groups that consist of disks of different types and capacities. Storage pools enable easier storage space management and features such as snapshots.
Volume	A portion of storage space that is used to divide up and manage space on the NAS.	You can create volumes by dividing up storage pool space, or using the space of a RAID group. QTS offers three different volume types, with different combinations of performance and flexibility.  Important You must create at least one volume before the NAS can start storing data.

Object	Description	Details
iSCSI LUN (logical unit number)	A portion of storage space that can be used by other NAS devices, servers and desktop computers using the iSCSI protocol.	QTS offers two LUN types. - Block-based LUN: Created from a storage pool. It is similar to a volume, except that it has no file system and must be linked to an iSCSI host. - File-based LUN: Created on a volume. It is similar to an ISO image file.
Shared folder	A folder that is used for storing and sharing files.	Shared folders are created on volumes. QTS automatically creates a set of default shared folders. You can create more shared folders and configure permissions for each.

Global Settings

You can access global settings by clicking  in the **Storage & Snapshots** window.

Storage Global Settings

Setting	Description
RAID Resync Priority	Specify the minimum speed of the following RAID operations: - Rebuild - Migration - Scrubbing - Sync You can select one of the following priorities: Service First: QTS performs RAID operations at lower speeds in order to maintain NAS storage performance. Default: QTS performs RAID operations at the default speed. Resync First: QTS performs RAID operations at higher speeds. Users may notice a decrease in NAS storage performance while RAID operations are in progress.  Important This setting only affects RAID operation speeds when the NAS is in use. When the NAS is idle, all RAID operations are performed at the highest possible speeds.
RAID Scrubbing Schedule	Enable this feature to periodically scan for and fix bad sectors on RAID 5 and RAID 6 groups. For details, see Running RAID Scrubbing on a Schedule.

Setting	Description
Auto Reclaim and SSD Trim Schedule	Enable this feature to periodically run the following operations on all thin volumes and SSDs: • Auto Reclaim: QTS returns unused storage space to the parent storage pool when files are deleted from thin volumes. • SSD Trim: QTS tells the SSD firmware which data blocks it is safe to erase when performing garbage collection. This helps maintain the SSD's write performance and lifespan. By default, the operations are scheduled to run daily at 2:00 AM. SSD Trim is only performed on solid state drives that belong to a RAID 0, RAID 1, or RAID 10 group.  Tip You should enable this feature if you have one or more of the following storage items: • Thin volumes • SSD RAID groups of type: Single, RAID 0, RAID 1, RAID 10  Note To reclaim space on a thin LUN, the reclaim must be run on the iSCSI client.

Disk Health Global Settings

Setting	Description
Activate Predictive S.M.A.R.T. Migration	Enable this feature to regularly monitor disk health. If S.M.A.R.T. errors are detected on a disk, QTS displays a warning and then begins migrating data from the faulty disk to a spare disk. After the migration is finished, the healthy disk is used in place of the faulty disk. This process is safer than manually initiating a full RAID rebuild after a disk has failed.
S.M.A.R.T. polling time	Specify how often QTS checks disks for S.M.A.R.T. errors in minutes.
Disk Temperature Alarm	Enable this feature to monitor the disk temperatures. QTS displays a warning when the disk temperature is equal to or above the specified threshold. You can set separate thresholds for hard disk drives and solid state drives.

Setting	Description
TLER/ERC Timer	Enable this feature to specify a maximum response time of all disks in seconds. When a disk encounters a read or write error, it may become unresponsive while the disk firmware attempts to correct the error. QTS might interpret this unresponsiveness as a disk failure. Enabling this feature ensures that a disk has sufficient time to recover from a read or write error before QTS marks it as failed and initiates a RAID group rebuild.  Tip - This setting is also known as Error recovery control (ERC), Time-limited error recovery (TLER) or Command completion time limit (CCTL). - When this feature is disabled, QTS uses the default TLER/ERC settings specified by the disk manufacturer.

Snapshot Global Settings

Setting	Description
Smart Snapshot Space Management	Enable this feature to automatically delete the oldest snapshots when the available snapshot storage space (guaranteed snapshot space plus free storage pool space) is less than 32GB. You can choose to exclude the most recent snapshot, or snapshots that were created with the setting Keep this snapshot permanently.  Important If QTS is unable to create 32GB of free snapshot space, it will not create any new snapshots.
Enable File Station Snapshot Directory for administrators	Enable this feature to consolidate all available snapshots into a centralized folder in File Station. You can restore files and folders from the snapshot directory by copying them into another folder.
Make snapshot directory (@Recently-Snapshot) visible in shared folder root	Enable this feature to show a read-only folder @Recently-Snapshot at the root level of each shared folder, containing all of the shared folder's snapshots. You can restore files and folders from @Recently-Snapshot by copying them into another folder.
When the number of snapshots reaches maximum	Specify the default QTS behavior after a volume, LUN, or NAS reaches its maximum number of snapshots. You can choose one of the following behaviors: - Overwrite the oldest snapshot when taking a new one. - Stop taking snapshots. The maximum number of snapshots depends on your NAS model. .
Use timezone GMT+0 for all new snapshots	Enable this feature to use the GMT+0 time zone in the file names of new snapshots. This file naming convention can simplify snapshot management especially when working with snapshots from NAS devices located in different time zones. This setting only applies to new snapshots. Existing snapshots are not renamed.
Show hidden files in Snapshot Manager	Enable this feature to display hidden files in Snapshot Manager. This setting does not affect files inside the File Station Snapshot Directory.

Setting	Description
Enable Windows Previous Versions	When enabled, Windows users can view and restore files from snapshots using the Previous Versions feature in Windows. You can disable this feature for individual folders by modifying the folder's properties.

Storage

QTS provides a flexible volume architecture that enables you to easily manage, store, and share files.

Disks

Disk Types

QTS restricts which type of disk can be used to create SSD cache, storage pools, and static volumes.



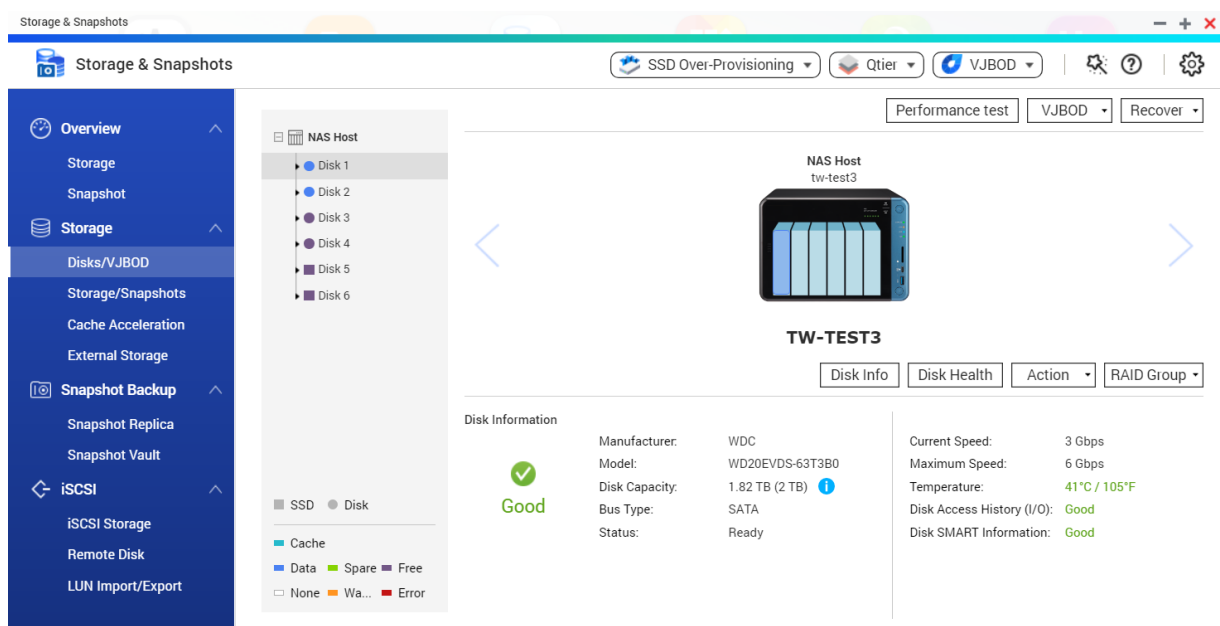
Important

Existing storage pools and static volumes configured on PCIe M.2 and PCIe form-factor SSDs will not be affected after updating to QTS 4.4.

Disk Type	Installation Method	SSD Cache	Storage Pools/Static Volumes
SATA/SAS/NL-SAS 3.5" HDD	NAS drive bay	No	Yes
SATA/SAS 2.5" HDD	NAS drive bay	No	Yes
SATA/SAS 2.5" SSD	NAS drive bay	Yes	Yes
PCIe NVMe M.2 SSD	QM2 card	Yes	Yes
PCIe NVMe M.2 SSD	3rd-party M.2 to PCIe adapter card	Yes	No
SATA M.2 SSD	QM2 card	Yes	Yes
SATA M.2 SSD	NAS internal M.2 slot	Yes	Yes
PCIe form-factor SSD	PCIe slot	Yes	No

Disk Management

You can manage disks at **Main Menu > Storage & Snapshots > Storage > Disks/VJBOD**.



Disk Status Information

Status	Color	Description
Cache		The disk is used as an SSD cache.
Data		The disk contains data and is part of a static volume or storage pool.
Spare		The disk is configured as a hot spare. For details, see RAID Spare Disks .
Free		The disk is not in use.
None		There is no disk in the drive bay.
Warning		QTS has detected S.M.A.R.T. errors. Run a full S.M.A.R.T. test and a disk scan.
Error		QTS has detected I/O errors. You must replace the disk immediately.

Disk Actions

Selecting a disk on the **Disks/VJBOD** screen enables you to view its status and general hardware details.

Action	Description
Disk Info	View disk details, including the disk manufacturer, model, serial number, disk capacity, bus type, firmware version, ATA version and ATA standard.
Disk Health	View disk S.M.A.R.T information. For details, see Disk Health Information .

Action	Description
Scan Now	Scan the disk for bad blocks.  Tip Run this scan if the disk's status changes to Warning or Error. If QTS does not detect any bad blocks, the status changes back to Ready. To view the number of bad blocks, see Disk Health > Summary.
Locate	Prompt the drive LEDs to blink so that you can locate the drive in a NAS or expansion unit.
Detach	Remove the disk from its RAID group. The group must be of type: RAID 1, RAID 5, RAID 6, RAID 10.
Set as Enclosure Spare	Assign the disk as a global hot spare for all RAID groups within the same enclosure (NAS or expansion unit). For details, see Configuring a Global Hot Spare .
Disable Spare	Unassign the disk as a global hot spare.
New Volume	Create a new volume. For details, see Volume Creation .
Secure Erase	Permanently erase all data on a disk. For details, see Secure Erase .
RAID Group	Select a RAID group to view its RAID type, capacity, and member disks.

Disk Health Information

Tab	Description	Actions
Summary	Displays an overview of S.M.A.R.T. disk information and the results from the most recent disk scan and S.M.A.R.T. test.	No actions
SSD Features List	Displays all supported SSD ATA features.	No actions
SMART Information	Displays S.M.A.R.T. disk information and supported attributes.	No actions
Test	Run a S.M.A.R.T. disk self-test.	Select one of the following options: • Rapid Test: Tests the electrical and mechanical properties of the disk, and a small portion of the disk surface. The test takes approximately one minute. • Complete Test: Tests the electrical and mechanical properties of the disk, and the full disk surface. This test duration varies depending on the storage environment.

Tab	Description	Actions
Settings	Disk settings can be applied individually, or to multiple disks at once.	Configure the following settings: • Enable temperature alarm: QTS displays a warning when the disk temperature is equal to or above the specified threshold. • S.M.A.R.T. Test schedule: Schedule periodic rapid and complete S.M.A.R.T. disk tests. The results are displayed on the Summary screen.  Tip You can apply these settings to the current disk, all disks, or to disks with the same type as the current disk (HDD or SSD).

Disk Performance Tests

QTS can test the sequential and random read speeds of your disks.



Important

- The results provided by these tests are specific to the NAS being tested.
- For accurate results, do not use any resource-intensive applications while the tests are running.

Testing Disk Performance

1. Go to **Main Menu > Storage & Snapshots > Storage > Disks/VJBOD**.
2. Click **Performance Test**.
The **Performance Test** screen appears.
3. Select one or more disks.
4. Click **Performance Test** and then select a test type.

Test Type	Description	Test Results Format
Sequential read	Test sequential read speed.	MB/s
IOPS read	Test random read speed.	IOPS

A confirmation message appears.

5. Click **OK**.

6. Optional: Schedule a weekly sequential read test for all disks. The weekly test runs every Monday at 6:30 AM.

- a. Click **Weekly Test**.

- b. Click **OK**.

QTS runs the test and then displays the results on the **Performance Test** screen. To see detailed results for the IOPS read test, select one or more disks and then select **Result > IOPS read result**.

Secure Erase

Secure erase permanently deletes all data on a disk, ensuring that the data is unrecoverable. Using secure erase on an SSD also restores the disk's performance to its original factory state.

Securely Erasing a Disk



Important

Do not disconnect any disks or power off the NAS while secure erase is running.

1. Go to **Main Menu > Storage & Snapshots > Storage > Disks/VJBOD**.
2. Select a free disk.
3. Select **Action > Secure Erase**.
The **Secure Erase** window opens.
4. Optional: Select additional disks to erase.
5. Click **Next**.
6. Select an erase mode.

Mode	Description
Complete	QTS writes over all blocks on the disk with zeros or ones. This mode is the most secure but can take a long time to finish. Select Customized to configure the following the erase settings. • Number of rounds: QTS writes over all blocks on the disk the specified number of times. • Overwrite with: Overwrite all blocks with zeros, ones, or a random zero or one.
SSD	QTS issues a solid state drive (SSD) secure erase ATA command. The SSD firmware then erases all data and restores the disk to its original factory performance.  Important This feature is only supported on specific SSD models.
Fast	QTS overwrites the partition and RAID configuration data on the disk with zeros. This mode is the quickest but is less secure than the other modes.

7. Click **Next**.
8. Enter the administrator password.
9. Click **Apply**.

QTS starts erasing the disk. You can monitor the progress in **Background Tasks**.

Volumes

A volume is a storage space created from a storage pool or RAID group. Volumes are used to divide and manage your NAS storage space.



Tip

- QTS supports the creation of three types of volume. For more information, see [Thick](#), [Thin](#), and [Static Volumes](#).
- When organizing your storage space, you can either create one large volume or multiple smaller volumes. For more information, see [Volume Configuration](#).

Volume Types

Thick, Thin, and Static Volumes

	Volume Type		
	Static	Thick	Thin
Summary	Best overall read/write performance, but does not support most advanced features	Good balance between performance and flexibility	Enables you to allocate storage space more efficiently
Read/write speed	Fastest for random writes	Good	Good
Flexibility	Inflexible A volume can only be expanded by adding extra drives to the NAS.	Flexible A volume can easily be resized.	Very flexible A volume can be resized. Also unused space can be reclaimed and added back into the parent storage pool.
Parent storage space	RAID group	Storage pool	Storage pool
Volumes allowed in parent storage space	One	One or more	One or more
Initial size	Size of the parent RAID group	User-specified	Zero Storage pool space is allocated on-demand, as data is written to the volume. This is called thin provisioning.
Maximum size	Size of the parent RAID group	Size of the parent storage pool	Twenty times the amount of free space in the parent storage pool The size of a thin volume can be greater than that of its parent storage pool. This is called over-allocation.
Effect of data deletion	Space is freed in the volume	Space is freed in the volume	QTS can reclaim the space and add it back into the parent storage pool.

	Volume Type		
	Static	Thick	Thin
Method of adding storage space	- Add disks to the NAS - Replace existing disks with higher capacity disks	Allocate more space from the parent storage pool	Allocate more space from the parent storage pool
Snapshot support (fast backup and recovery)	No	Yes	Yes
Qtier (automatic data tiering) support	No	Yes	Yes

Legacy Volumes

A legacy volume is a volume created in QTS 3.x or earlier, before QTS had storage pools. A NAS will contain legacy volumes in the following situations:

- A volume was created on a NAS running QTS 3.x or earlier, and then the NAS was updated to QTS 4.0 or later.
- A volume was created on a NAS running QTS 3.x or earlier, and then the disks containing the volume were moved to a different NAS running QTS 4.0 or later.

You can use legacy volumes for data storage, but their behavior and status will not be consistent with other volume types. They also cannot use newer QTS features such as snapshots.



Tip

QNAP recommends replacing legacy volumes with newer volumes. To replace a legacy volume, back up all data, create a new thick, thin, or static volume, and then restore the data to the new volume.

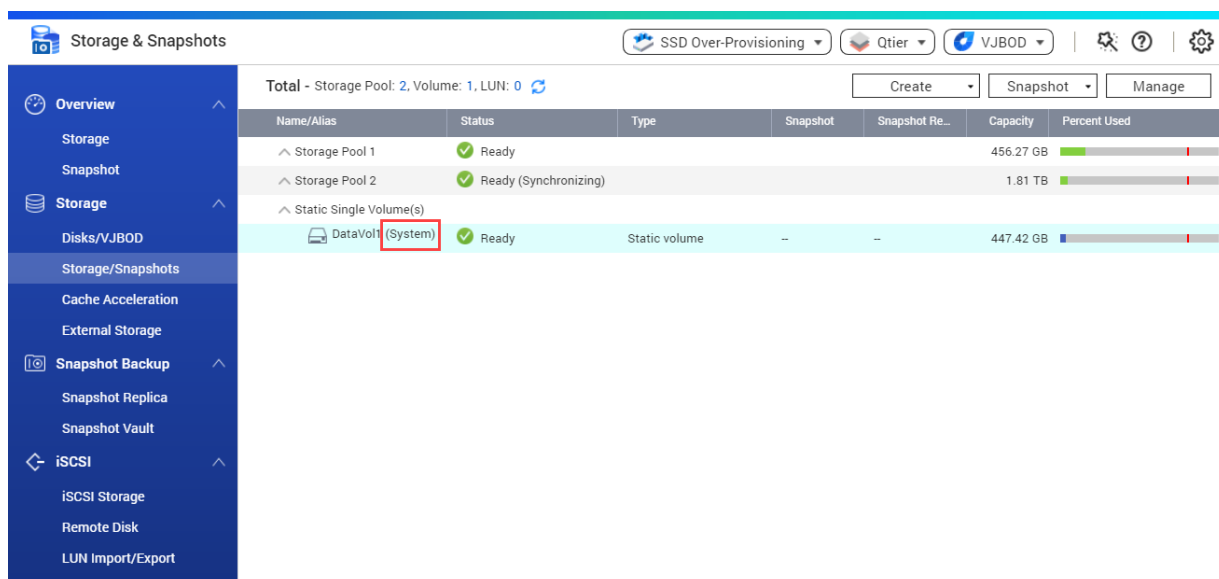
The System Volume

The system volume is a regular static or thick volume that QTS uses to store system data such as logs, metadata, and thumbnails. By default, applications are installed to the system volume. If no system volume exists, either because the NAS has recently been initialized or the system volume was deleted, QTS will assign the next static or thick volume that you create as the system volume.



Important

QNAP recommends creating a system volume of at least 10GB. This is to prevent errors caused by insufficient system volume space



Volume Configuration

Volumes divide the NAS storage space into separate areas. You can create one large volume or multiple smaller volumes. Each volume can contain one or more shared folders, which are used to store and share files.

Configuration	Advantage	Description
Single Volume Example: - Volume 1 - Shared Folder 1 - Shared Folder 2 - Shared Folder 3 - Shared Folder 4	Simplicity	Creating one volume is quick and easy. After the initial setup, you do not have to worry about changing volume sizes or creating new volumes.
	Speed	Single static volumes are faster because they do not require a storage pool.

Configuration	Advantage	Description
Multiple Volumes Example: • Volume 1 • Shared Folder 1 • Volume 2 • Shared Folder 2 • Volume 3 • Shared Folder 3 • Shared Folder 4	Storage space limits	Each volume functions like a separate container. If a user or an app writes a large amount of files to a volume, only the specified volume is filled. Other volumes remain unaffected.
	Multiple snapshot schedules	Snapshots protect files from accidental deletion or modification. Snapshot creation requires time, memory resources, and storage space. QTS takes snapshots of individual volumes. Using multiple volumes means you can have different snapshot schedules for different file types. For example, you can take hourly snapshots of the volume containing important documents, and weekly snapshots of the volume contain photos and movies.
	Faster file system repair	In certain circumstances such as after a power outage, QTS may encounters errors in the file system of a volume. While QTS can scan the volume and automatically repair errors, this process can take a long time. The required time depends on the volume size. Files on the volume cannot be accessed during the scanning process.

Volume Configuration Examples

Users often purchase NAS devices to store a combination of documents, media, and backups.

The following table compares the advantages and disadvantages of creating a single large volume or multiple smaller volumes.

Requirement	User Goal	Single Volume	Multiple Volumes
Simplicity	Store files	Users create one large thin volume if they want to use snapshots, or one large static volume if they do not. They then create three shared folders on the volume, for documents, movies, and backups.	Users create three separate volumes for documents, movies, and backups. Users must decide how much space to initially allocate to each volume.
Speed	Edit video and audio files	Users create one large single static volume on the NAS. The files are backed up daily to another NAS, or to an external disk.	Users create a thick volume to store the movies files. Random-write performance is slightly lower than a single static volume.
Containerizing storage space	Copy a large number of movie files to the NAS	Users copy the movie files to the movies shared folder. However, they must pay attention to much data they have in the movies folder. If they copy too many files, the volume will become full.	Users copy the movie files to the movies volume. When the volume becomes full, they can increase the volume size.

Requirement	User Goal	Single Volume	Multiple Volumes
Multiple snapshot schedules	Protect document files using snapshots	Users create a daily snapshot schedule for a single volume. The snapshots record all changes made to document files. However, the snapshots also record changes to movie and backup files which wastes resources and storage space.	Users create a daily snapshot schedule for the document volume only.
File system repair	Fix file system errors	QTS must scan the entire single volume, which can take a long time. The volume cannot be accessed during the scanning process, making the entire NAS unusable.	QTS only needs to scan the volume that has an error. Each volume is small, so scanning is relatively quick. Users can still access files on other volumes while the scan is in progress.

Volume Creation

Creating a Single Static Volume

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Perform one of the following actions.

NAS State	Action
No volumes or storage pools	Click New Volume .
One or more volumes or storage pools	Click Create > New Volume .

The **Volume Creation Wizard** window opens.

3. Select **Static Volume**.
4. Click **Next**.
5. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

- You cannot select disks from multiple expansion units.
- If the expansion unit is disconnected from the NAS, the storage pool will become inaccessible until it is reconnected.

6. Select one or more disks.
7. Select a RAID type.
QTS displays all available RAID types and automatically selects the most optimized RAID type.

Number of disks	Supported RAID Types	Default RAID Type
One	Single	Single
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5

Number of disks	Supported RAID Types	Default RAID Type
Four	JBOD, RAID 0, RAID 5, RAID 6, RAID 10  Important RAID 10 requires an even number of disks.	RAID 5
Five	JBOD, RAID 0, RAID 5, RAID 6	RAID 6
Six or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50	RAID 6
Eight or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60	RAID 6

**Tip**

Use the default RAID type if you are unfamiliar with the technology.
For details, see [RAID Types](#).

8. Optional: Select the disk that will be used as a hot spare for this RAID group.
The designated hot spare automatically replaces any disk in the RAID group that fails.
For details, see [RAID Spare Disks](#).
9. Optional: Select the number of RAID 50 or RAID 60 sub-groups.
The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.
 - A higher number of sub-groups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
 - A lower number of sub-groups results in more storage capacity, and better performance if all the disks are HDDs.

**Warning**

If a RAID group is divided unevenly, the excess space becomes unavailable. For example, 10 disks divided into 3 sub-groups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

10. Click **Next**.
11. Optional: Specify an alias for the volume.
The alias must consist of 1 to 64 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Hyphen "-" and underscore "_"
12. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

13. Specify the number of bytes per inode.
The number of bytes per inode determines the maximum volume size, and the number of files and folders that the volume can store. Increasing the number of bytes per inode results in a larger maximum volume size, but a lower maximum number of files and folders.

14. Optional: Configure advanced settings.

Setting	Description	User Actions
Alert threshold	QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.	Specify a value.
Encryption	QTS encrypts all data on the volume with 256-bit AES encryption.	- Specify an encryption password containing 8 to 32 characters, with any combination of letters, numbers and special characters. Spaces are not allowed. - Select Save encryption key to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.  Warning - Saving the encryption key on the NAS can result in unauthorized data access if unauthorized personnel are able to physically access the NAS. - If you forget the encryption password, the volume will become inaccessible and all data will be lost.
Accelerate performance with SSD cache	QTS adds data from this volume to the SSD cache to improve read or write performance.	No actions
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder.	- Specify a folder name. - Select Create this folder as a snapshot shared folder. A snapshot shared folder enables faster snapshot creation and restoration.

15. Click **Next**.

16. Click **Finish**.
A confirmation message appears.


Warning
 Clicking **OK** deletes all data on the selected disks.

QTS creates and initializes the volume, and then creates the optional shared folder.

Creating a Thick or Thin Multiple Volume

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Perform one of the following actions.

NAS State	Action
No volumes or storage pools	Click New Volume .
One or more volumes or storage pools	Click Create > New Volume .

The **Volume Creation Wizard** window opens.

3. Select the volume type.

- Thick Volume
- Thin Volume

For details, see [Volumes](#).

4. Select a storage pool.
You can select an existing storage pool or create a new storage pool immediately.
5. Optional: Create a new storage pool.

- a. Click .

The **Create Storage Pool Wizard** window opens.

- b. Click **Next**.

- c. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

- You cannot select disks from multiple expansion units.
- If the expansion unit is disconnected from the NAS, the storage pool will become inaccessible until it is reconnected.

- d. Select one or more disks.



Warning

All data on the selected disks will be deleted.

- e. Select a RAID type.
QTS displays all available RAID types and automatically selects the most optimized RAID type.

Number of disks	Supported RAID Types	Default RAID Type
One	Single	Single
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5
Four	JBOD, RAID 0, RAID 5, RAID 6, RAID 10	RAID 5
Five	JBOD, RAID 0, RAID 5, RAID 6	RAID 6

Number of disks	Supported RAID Types	Default RAID Type
Six or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50  Note RAID 10 requires an even number of disks.	RAID 6
Eight or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60	RAID 6

**Tip**

Use the default RAID type if you are unfamiliar with the technology.
For details, see [RAID Types](#).

- f. Optional: Select the disk that will be used as a hot spare for this RAID group.
The designated hot spare automatically replaces any disk in the RAID group that fails.
For RAID 50 or RAID 60, a spare disk must be configured later. You should configure a global spare disk so that all sub-groups share the same spare disk. For details, see [Configuring a Global Hot Spare](#).
- g. Click **Next**.
- h. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

- i. Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
- j. Click **Next**.
- k. Verify the storage pool information.
- l. Click **Create**.
A confirmation message appears.

**Warning**

Clicking **OK** deletes all data on the selected disks.

- m. Click **OK**.

QTS creates the storage pool. The **Create Storage Pool Wizard** window closes.

6. Click **Next**.

7. Optional: Specify an alias for the volume.
The alias must consist of 1 to 64 characters from any of the following groups:

- Letters: A to Z, a to z
- Numbers: 0 to 9
- Special characters: Hyphen "-" and underscore "_"

8. Specify the capacity of the volume.

The volume type determines the maximum volume capacity.

Volume Type	Maximum Size
Thick	Amount of free space in the parent storage pool.
Thin	Twenty times the amount of free space in the parent storage pool

Setting the maximum size of a thin volume to a value that is greater than the amount of free space in the storage pool is called over-allocation.

9. Specify the number of bytes per inode.

The number of bytes per inode determines the maximum volume size, and the number of files and folders that the volume can store. Increasing the number of bytes per inode results in a larger maximum volume size, but a lower maximum number of files and folders.

10. Optional: Configure advanced settings.

Setting	Description	User Actions
Alert threshold	QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.	Specify a value.
Encryption	QTS encrypts all data on the volume with 256-bit AES encryption.	- Specify an encryption password containing 8 to 32 characters, with any combination of letters, numbers and special characters. Spaces are not allowed. - Select Save encryption key to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.  Warning - Saving the encryption key on the NAS can result in unauthorized data access if unauthorized personnel are able to physically access the NAS. - If you forget the encryption password, the volume will become inaccessible and all data will be lost.
Accelerate performance with SSD cache	QTS adds data from this volume to the SSD cache to improve read or write performance.	

Setting	Description	User Actions
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder.	- Specify a folder name. - Select Create this folder as a snapshot shared folder. A snapshot shared folder enables faster snapshot creation and restoration.

11. Click **Next**.

12. Click **Finish**.

QTS creates and initializes the volume, and then creates the optional shared folder.

Volume Management

Deleting a Volume

- Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
- Select a volume.



Warning

All data on the selected volume will be deleted.

- Click **Manage**.
- Select **Remove > Remove Volume**.
The **Volume Removal Wizard** window opens.
- Click **Apply**.

Configuring a Volume Space Alert

- Go to **Main Menu > Storage & Snapshots**.
- Select a volume.
- Click **Manage**.
- Select **Actions > Set Threshold**.
- Enable or disable volume space alerts.
- Specify an alert threshold.
QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.
- Click **Apply**.

Volume Expansion

Expanding a volume increases its maximum capacity so that it can store more data.

Resizing a Thick or Thin Volume

The maximum capacity of thick and thin volumes can be increased or decreased.

Operation	Details
Expand Volume	- The operation can be performed while the volume is online and accessible to users. - For a thick volume, additional space is allocated from the volume's parent storage pool.
Shrink Volume	- Users and applications will be unable to access the volume until the operation is finished. - For a thick volume, the freed space is returned to the volume's parent storage pool.

Volume Type	Maximum Allowed Capacity
Thick	Amount of free space in the parent storage pool.
Thin	Twenty times the amount of free space in the parent storage pool.  Important Setting the maximum size of a thin volume to a value that is greater than the amount of free space in the storage pool is called over-allocation.

- Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
- Select a thick or thin volume.
- Click **Manage**.
- Click **Resize Volume**.
The **Volume Resizing Wizard** opens.
- Specify a new capacity for the volume.
Capacity can be specified in megabytes (MB), gigabytes (GB) or terabytes (TB).
- Optional: Click **Set to Max**.
Sets the new volume capacity to the maximum available size. This option is only available for thick volumes.
- Click **Apply**.
If you are shrinking the volume, a confirmation message appears.
- Click **OK**.
The **Volume Resizing Wizard** closes. The volume status changes to *Expanding...* or *Shrinking...*

After expansion is complete, the volume status changes back to *Ready*.

Expanding a Static Volume by Adding Disks to a RAID Group

The total storage capacity of a static volume can be expanded by adding one or more additional disks to a RAID group in the static volume. This extra capacity can be added online, without any interruption to data access.

**Important**

- Adding disks to a RAID 1 group changes the RAID type of the group to RAID 5.
- To expand a RAID 50 or RAID 60 group, every sub-group must be expanded with the same number of disks.

1. Verify the following:
 - The storage pool you want to expand contains at least one RAID group of type: RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60.
 - The NAS contains one or more free disks. Each free disk must be the same type as the other disks in the RAID group (either HDD or SSD), and have a capacity that is equal to or greater than the smallest disk in the group.
 - The status of the RAID group that you want to expand is *Ready*.
2. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
3. Select a static volume.
4. Click **Manage**.
The **Volume Management** window opens.
5. Click **Expand**.
The **Expand Static Volume Wizard** window opens.
6. Select **Add new disk(s) to an existing RAID group**.
7. Select a RAID group.
The group must be of type: RAID 1, RAID 5, RAID 6, RAID 50, RAID 60.
8. Click **Next**.
9. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

10. Click **Next**.
11. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

12. Click **Next**.
13. Click **Expand**.
A confirmation message appears.
14. Click **OK**.
15. Optional: For a RAID 50 or RAID 60 volume, repeat these steps for each sub-group.

QTS starts rebuilding the RAID group. The storage capacity of the volume increases after RAID rebuilding is finished.

Expanding a Single Static Volume By Adding a New RAID Group

The storage capacity of a static volume can be expanded by creating a new RAID group and then adding it to the volume. This operation can be performed while the volume is online and accessible to users. QTS writes data linearly to storage pools containing multiple RAID groups. This means that it writes data to a RAID group until it is full before writing data to the next RAID group.



Warning

- If a static volume contains multiple RAID groups and one RAID group fails, all data on the volume will be lost. Ensure that you have a complete data backup plan.
- To expand a RAID 50 or RAID 60 pool, you must create a new RAID 50 or 60 group with the same number of disks and sub-groups as the original pool. It is not possible to add additional sub-groups.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a static volume.
3. Click **Manage**.
The **Volume Management** window opens.
4. Click **Expand**.
The **Expanding Static Volume Wizard** window opens.
5. Select **Create and add a new RAID group**.
6. Click **Next**.
7. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

If the expansion unit is disconnected from the NAS, the storage pool will become inaccessible until it is reconnected.

8. Select one or more disks.



Warning

All data on the selected disks will be deleted.

9. Select a RAID type.
QTS displays all available RAID types and automatically selects the most optimized RAID type.



Important

- If the storage pool contains a RAID 1, RAID 5, RAID 6 or RAID 10 group, the new RAID group must also have one of the mentioned RAID types.
- For RAID 50 or RAID 60, you cannot select a different RAID type.

10. Optional: Select the disk that will be used as a hot spare for this RAID group.
For details, see [Configuring a RAID Group Hot Spare](#).
11. Click **Next**.

12. Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.


Tip

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

13. Click **Next**.
14. Click **Expand**.
A confirmation message appears.
15. Click **OK**.

QTS creates the new RAID group and then starts rebuilding the volume. The capacity of the volume increases after RAID rebuilding is finished.

Storage Pools

A storage pool aggregates many physical disks into one large storage space. Disks are joined together using [RAID](#) technology to form a RAID group. Storage pools may contain more than one RAID group. Using a storage pool provides the following benefits:

- Multiple volumes can be created on a storage pool, enabling you to divide the storage space among different users and applications.
- Disks of different sizes and types can be mixed into one large storage space.
- Disks from connected expansion units can be mixed with disks in the NAS to form a storage pool.
- Extra disks can be added while the storage pool is in use, increasing storage capacity without interrupting services.
- Qtier provides auto-tiering when a storage pool contains a mix of SATA, SAS, and SSD disks. Qtier automatically moves frequently accessed hot data to the faster SSDs, and infrequently accessed cold data to the slower disks.
- Snapshots can only be used with storage pools. Snapshots record the state of the data on a volume or LUN at a specific point in time. Data can then be restored to that time if it is accidentally modified or deleted.
- Multiple RAID 5 or RAID 6 can be striped together to form a RAID 50 or RAID 60 pool.

Creating a Storage Pool

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Perform one of the following actions.

NAS State	Action
No volumes or storage pools	Click New Storage Pool
One or more volumes or storage pools	Click Create > New Storage Pool

The **Create Storage Pool Wizard** window opens.

3. Click **Next**.

4. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

- You cannot select disks from multiple expansion units.
- If the expansion unit is disconnected from the NAS, the storage pool will become inaccessible until it is reconnected.

5. Select one or more disks.



Warning

All data on the selected disks will be deleted.

6. Select a RAID type.

QTS displays all available RAID types and automatically selects the most optimized RAID type.

Number of disks	Supported RAID Types	Default RAID Type
One	Single	Single
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5
Four	JBOD, RAID 0, RAID 5, RAID 6, RAID 10	RAID 5
Five	JBOD, RAID 0, RAID 5, RAID 6	RAID 6
Six or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50	RAID 6
	 Note RAID 10 requires an even number of disks.	
Eight or more	JBOD, RAID 0, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60	RAID 6



Tip

Use the default RAID type if you are unfamiliar with the technology.
For details, see [RAID Types](#).

7. Optional: Select the disk that will be used as a hot spare for this RAID group.

The designated hot spare automatically replaces any disk in the RAID group that fails.

For RAID 50 or RAID 60, a spare disk must be configured later. You should configure a global spare disk so that all sub-groups share the same spare disk. For details, see [Configuring a Global Hot Spare](#).

8. Optional: Select the number of RAID 50 or RAID 60 sub-groups.

The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.

- A higher number of sub-groups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
- A lower number of sub-groups results in more storage capacity, and better performance if all the disks are HDDs.



Warning

If a RAID group is divided unevenly, the excess space becomes unavailable. For example, 10 disks divided into 3 sub-groups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

9. Click **Next**.
10. Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

11. Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
12. Click **Next**.
13. Click **Create**.
A confirmation message appears.
14. Click **OK**.

QTS creates the storage pool and then displays the information on the **Storage/Snapshot** screen.

Deleting a Storage Pool

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a storage pool.

**Warning**

All data in the storage pool will be deleted.

3. Click **Manage**.
4. Select **Remove > Remove Pool**.
A notification window opens.
5. Select **Confirm the removal of every volume/iSCSI LUN/Snapshot Vault on this storage pool**.
6. Click **OK**.
7. Enter your password.
8. Click **OK**.

Configuring a Storage Pool Alert Threshold

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a storage pool.
3. Click **Manage**.
4. Select **Actions > Set Threshold**.
5. Enable or disable volume space alerts.
6. Specify an alert threshold.

QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.

7. Click **Apply**.

Storage Pool Expansion

Expanding a Storage Pool by Adding Disks to a RAID Group

The total storage capacity of a storage pool can be expanded by adding one or more additional disks to a RAID group. This operation can be performed while the pool is online and accessible to users.



Important

- Adding disks to a RAID 1 group changes the RAID type of the group to RAID 5.
- To expand a RAID 50 or RAID 60 group, every sub-group must be expanded with the same number of disks.

1. Verify the following:
 - The storage pool you want to expand contains at least one RAID group of type: RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60.
 - The NAS contains one or more free disks. Each free disk must be the same type as the other disks in the RAID group (either HDD or SSD), and have a capacity that is equal to or greater than the smallest disk in the group.
 - The status of the RAID group that you want to expand is *Ready*.
2. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
3. Select a storage pool.
4. Click **Manage**.
The **Storage Pool Management** window opens.
5. Select **Expand Pool > Expand Pool**.
The **Expanding Storage Pool Wizard** window opens.
6. Select **Add new disk(s) to an existing RAID group**.
7. Select a RAID group.
The group must be of type: RAID 1, RAID 5, RAID 6, RAID 50, RAID 60.
8. Click **Next**.
9. Select one or more disks.



Warning

All data on the selected disks will be deleted.

10. Click **Next**.
11. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

12. Click **Next**.
13. Click **Expand**.
A confirmation message appears.
14. Click **OK**.
15. Optional: For a RAID 50 or RAID 60 pool, repeat these steps for each sub-group.

QTS starts rebuilding the RAID group. The storage capacity of the pool increases after RAID rebuilding is finished.

Expanding a Storage Pool By Adding a New RAID Group

The storage capacity of a storage pool can be expanded by creating a new RAID group and then adding it to the pool. This operation can be performed while the pool is online and accessible to users. QTS writes data linearly to storage pools containing multiple RAID groups. This means that it writes data to a RAID group until it is full before writing data to the next RAID group.

**Warning**

- If a storage pool contains multiple RAID groups and one RAID group fails, all data in the storage pool will be lost. Ensure that you have a complete data backup plan.
- To expand a RAID 50 or RAID 60 pool, you must create a new RAID 50 or 60 group with the same number of disks and sub-groups as the original pool. It is not possible to add additional sub-groups.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a storage pool.
3. Click **Manage**.
The **Storage Pool Management** window opens.
4. Select **Expand Pool > Expand Pool**.
The **Expand Storage Pool Wizard** window opens.
5. Select **Create and add a new RAID group**.
6. Click **Next**.
7. Optional: Select an expansion unit from the **Enclosure Unit** list.

**Important**

If the expansion unit is disconnected from the NAS, the storage pool will become inaccessible until it is reconnected.

8. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

9. Select a RAID type.
QTS displays all available RAID types and automatically selects the most optimized RAID type.

**Important**

- If the storage pool contains a RAID 1, RAID 5, RAID 6 or RAID 10 group, the new RAID group must also have one of the mentioned RAID types.
- For RAID 50 or RAID 60, you cannot select a different RAID type.

- Optional: Select the disk that will be used as a hot spare for this RAID group.
For details, see [Configuring a RAID Group Hot Spare](#).
- Click **Next**.
- Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

- Click **Next**.
- Click **Expand**.
A confirmation message appears.
- Click **OK**.

QTS creates the new RAID group and then starts rebuilding the storage pool. The capacity of the pool increases after RAID rebuilding is finished.

Storage Pool Roaming

Storage pool roaming enables you to safely remove a storage pool and move it to another QNAP NAS. The following data is retained:

- Files and folders
- Volumes and LUN configuration
- Snapshots

Moving a Storage Pool to a Different NAS

- Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
- Select a storage pool.
- Click **Manage**.
The **Storage Pool Management** window opens.
- Select **Remove > Safely Detach Pool**.
A confirmation message appears.
- Click **Yes**.
The storage pool status changes to *Safely Detaching...* After QTS has finished detaching the pool, it disappears from **Storage & Snapshots**.

6. Remove the drives containing the storage pool from the NAS.
7. Install the drives in the second NAS.
8. On the second NAS, go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
9. Select **Recover > Scan All Free Disks** .
A confirmation message appears.
10. Click **OK**.
QTS scans the disks and detects the storage pool.
11. Click **Apply**.

The storage pool and all volumes and LUNs appear in **Storage & Snapshots** on the second NAS.

RAID

Redundant array of independent disks (RAID) combines multiple physical disks into a single storage unit, and then distributes data across the disks in one of several predefined methods.

The following features make RAID ideal for use with data storage and NAS applications.

RAID Feature	Description	Advantages	Disadvantages
Grouping	Disks that are combined using RAID form a RAID group, which QTS considers one large logical disk.	Managing the storage space of one large disk is simpler and more efficient than multiple small disks.	Initial configuration can be more complicated.
Striping	Data is split into smaller pieces. Each piece is stored on a different disk in the RAID group. QTS can then access that data by reading from or writing to multiple disks simultaneously, increasing read and write speeds.	• Greater read/write speeds, compared to a single disk • Speeds can be increased further by adding disks	If one disk in the RAID group fails, and the RAID group has no redundancy, all data will be lost.
Redundancy	Each disk in the RAID group can store the following: • Complete copy of the stored data • Metadata that allows reconstruction of lost data	• Disks can fail or be removed from the RAID group without any loss of data • Users can access data while failed disks are being replaced	Total storage capacity of the RAID group is reduced.

RAID Types

QTS supports several RAID types. Each type provides a different combination of striping and redundancy.



- If disks with different capacities are combined in one RAID group, all disks function according to the capacity of the smallest disk. For example, if a RAID group contains five 2 TB disks and one 1 TB disk, QTS detects six 1 TB disks. QNAP recommends the following when mixing disks of different capacities.
 - Create a separate RAID group for each capacity.
 - Combine the RAID groups using storage pools.
- Using only one disk type (HDD, SSD, SAS) in a RAID group is recommended. If different types of disk are combined in one RAID group, the RAID group will function according to the speed of the slowest disk.

RAID Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
Single	1	0	Total disk capacity	• Uses a single disk for storage. • Provides no disk failure protection or performance benefits. • Suitable for single disk configurations that have a data backup plan in place.
JBOD (just a bunch of disks)	1 or more	0	Total combined disk capacity	• Combines disks together in a linear fashion. QTS writes data to a disk until it is full before writing to the next disk. • Uses the total capacity of all the disks. • Not a real RAID type. It provides no disk failure protection or performance benefits. • Unless you have a specific reason to use JBOD, RAID 0 should be used instead.
RAID 0	2 or more	0	Total combined disk capacity	• Disks are combined together using striping. • RAID 0 offers the fastest read/write speeds and uses the total capacity of all the disks. • Provides no disk failure protection. This RAID type must be paired with a data backup plan. • Recommended for high performance applications such as video editing.

RAID Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
RAID 1	2	1	Half of the total combined disk capacity	• An identical copy of data is stored on two disks. If either disk fails, data can still be read from the other disk. • Half of the total disk capacity is lost, in return for a high level of data protection. • Recommended for NAS devices with two disks.
RAID 5	3 or more	1	Total combined disk capacity minus 1 disk	• Data and parity information are striped across all disks. • One disk is used for parity. This means that if any one disk in the group fails, it can be replaced and the data on it can be restored. • Striping means read speeds are increased with each additional disk. • Recommended for a good balance between data protection and speed.
RAID 6	4 or more	2	Total combined disk capacity minus 2 disks	• Data and parity information are striped across all disks. • Same as RAID 5, but two disks are used for parity. This means that it protects against two disk failures, but the capacity of two disks are lost. • Recommended for business and general storage use. It provides high disk failure protection and read performance.
RAID 10	4 or more (even number required)	1 per pair of disks	Half of the total combined disk capacity	• Every two disks are paired using RAID 1 for failure protection. Then all pairs are striped together using RAID 0. • Excellent random read/write speeds and high failure protection, but half the total disk capacity is lost. • Recommended for application or database storage.

RAID Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
RAID 50	6 or more	1 per disk sub-group	Total combined disk capacity minus 1 disk per sub-group	- Multiple small RAID 5 groups are striped to form one RAID 50 group. - Better failure protection and faster rebuild times than RAID 5. More storage capacity than RAID 10. - Better random access performance than RAID 5 if all of the disks are SSDs. - Recommended for enterprise backup with ten or more disks.
RAID 60	8 or more	2 per disk sub-group	Total combined disk capacity minus 2 disks per sub-group	- Multiple small RAID 6 groups are striped to form one RAID 60 group. - Better failure protection and faster rebuild time than RAID 6. More storage capacity than RAID 10. - Better random access performance than RAID 6 if all of the disks are SSDs. - Recommended for business storage and online video editing with twelve or more disks.

RAID Spare Disks

Configuring a RAID Group Hot Spare

Assigning a hot spare gives extra protection against data loss. In normal conditions, a hot spare disk is unused and does not store any data. When a disk in the RAID group fails, the hot spare disk automatically replaces the faulty disk. QTS copies the data to the spare disk in a process called RAID rebuilding.

1. Verify that the NAS contains one or more free disks.
2. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
3. Select a storage pool or single static volume.
4. Click **Manage**.
5. Select a RAID 1, RAID 5, RAID 6, or RAID 10 group.
6. Select **Manage > Configure Spare Disk**.
7. Select one or more disks.



Warning

All data on the selected disks will be deleted.

8. Click **Apply**.
A confirmation message appears.
9. Click **OK**.

The spare disks are added to the RAID group. The disk appears as a green *Spare* in the disks summary at **Disks/VJBOD**.

Configuring a Global Hot Spare

A global spare disk acts as a hot spare for all RAID groups in a NAS or a connected expansion unit. Under normal conditions, the disk is unused and does not store any data. When a disk in any RAID group fails, the hot spare disk automatically replaces the faulty disk. QTS copies the data to the spare disk in a process called RAID rebuilding.



Important

Storage enclosures (the NAS and connected expansion units) cannot share global spare disks. A unique global hot spare disk must be assigned to each storage enclosure.

1. Go to **Main Menu > Storage & Snapshots > Disks/VJBOD**
2. Optional: Select a connected expansion unit.
3. Select a free disk.



Warning

All data on the selected disk will be deleted.

4. Select **Action > Set as Enclosure Spare**.
A confirmation message appears.
5. Click **OK**.

The disk appears as a green *Spare* on the **Disks/VJBOD** screen.

RAID Bitmaps

If a disk is temporarily disconnected from its RAID group and then reconnected, the RAID group must synchronize all of its data. This process may take a long time. If the RAID group has a bitmap then only changes that were made after the disk was disconnected need to be synchronized, greatly speeding up the process.

A disk can become temporarily disconnected in the following situations.

- A disk is accidentally removed from the NAS while the NAS is powered on.
- The NAS unexpectedly shuts down because of a hardware or software error.
- A user presses the power button for 10 seconds or disconnects the power cable while the NAS is powered on.



Important

- You can only create bitmaps for RAID 1, RAID 5, RAID 6, and RAID 10 groups.
- Enabling a RAID bitmap may slightly decrease the read and write performance of the RAID group.

- A bitmap improves synchronization time only if the same disk is disconnected then reconnected. Having a bitmap does not improve synchronization time when a new disk is added to the RAID group.

Creating a RAID Bitmap

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a storage pool or single static volume.
3. Click **Manage**.
4. Select a RAID 1, RAID 5, RAID 6, or RAID 10 group.
5. Select **Manage > Enable Bitmap** .
A confirmation message appears.

QTS creates a bitmap for the RAID group.

RAID Management

Expanding a RAID Group by Replacing all Disks

You can increase the maximum storage capacity of a RAID group by replacing all member disks with higher-capacity disks. This operation can be performed while the RAID group is online and accessible to users.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a storage pool or static volume.
3. Click **Manage**.
4. Select a RAID group of type: RAID 1, RAID 5, RAID 6, RAID 10.
5. Disable all hot spares and global hot spares assigned to the RAID group.
6. Select **Manage > Replace Disks One by One** .
7. Select a disk to replace.
Ensure that the capacity of the new disk is greater than the capacity of the disk that it is replacing.
8. Click **Change**.
The disk description changes to `Please remove this drive`.
9. Remove the disk from the NAS drive bay.
The NAS beeps twice. Then the disk description changes to `Please insert the new disk`.
10. Insert a new disk into the same bay.
The NAS beeps twice. Then the status of the disk and RAID group change to `Rebuilding`.
11. Wait for rebuilding to finish.



Warning

Do not remove any disks while the RAID group is rebuilding.

The disks status changes back to `Good`.

12. Repeat the previous steps until all disks in the RAID group have been replaced.
The **Expand Capacity** button is enabled after all disks have been replaced and rebuilding has finished.

13. Click **Expand Capacity.**

A confirmation message appears.

14. Click **OK.**

The NAS beeps and the RAID group status changes to *Synchronizing*.

**Warning**

Do not power off the NAS or remove any disks while synchronization is in progress.

The RAID group status changes to *Ready*.

Changing the RAID Type of a RAID Group

You can change the RAID type of an existing RAID group online, without losing access to data or any interruption to NAS services. Changing the RAID type of a RAID group is called RAID migration. QTS allows the following migrations.

Original RAID Type	New RAID Type	Additional Disks Required
Single	RAID 1	One
RAID 1	RAID 5	One or more
RAID 5	RAID 6	One or more

**Tip**

Migration from a single disk to RAID 6 is performed in stages. First migrate the group to RAID 1, then to RAID 5, and then finally to RAID 6.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Verify the following:
 - The NAS contains one or more available disks.
 - The capacity of each available disk is greater than or equal to the smallest disk in the RAID group.
3. Select a storage pool or static volume.
4. Click **Manage**.
5. Select a RAID group.
6. Select **Manage > Migrate**.
7. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

8. Click **Apply**.
A confirmation message appears.
9. Click **OK**.
The RAID group status changes to *Rebuilding...*

The RAID type changes to the new type and the RAID group status changes to *Ready* after migration has finished.

Recovering a RAID Group

RAID recovery enables you to recover a RAID group in the event of accidental disk removal or SATA connector failure. When several disks are removed or disconnected from a RAID group:

- The status of the group changes to `Error`.
- The statuses of all volumes and storage pools using the RAID group change to `Inactive`.
- All data on the affected volumes and LUNs becomes inaccessible.



Important

RAID recovery only helps when disks are temporarily disconnected and then reconnected. It does not help in the event of disk failure.

1. Reconnect all disconnected disks.



Important

Ensure that each disk is reinserted into its original drive bay.

2. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
3. Select a storage pool or single static volume with the status `Inactive`.
4. Click **Manage**.
5. Select a RAID group with the status `Error`.
6. Select **Manage > Recover**.

QTS starts to rebuild the RAID group.

RAID Scrubbing

RAID scrubbing helps maintain the consistency of data on the NAS. QTS scans the sectors of a RAID 5 or RAID 6 group and automatically attempts to repair any detected errors. You can run RAID scrubbing manually, or on a schedule.



Tip

QNAP recommends performing RAID scrubbing at least once a month to maintain system health and prevent data loss.

Running RAID Scrubbing Manually



Warning

The read/write speeds of the RAID group may decrease while RAID scrubbing is in progress.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a storage pool or static volume.
3. Click **Manage**.
4. Select a RAID 5 or RAID 6 group.
The RAID group status must be `Ready`.
5. Select **Manage > RAID Scrubbing**.

The RAID group status changes to *Scrubbing*.

Running RAID Scrubbing on a Schedule

You can schedule periodic RAID scrubbing of all RAID 5 and RAID 6 groups.



Warning

The read/write speeds of the RAID group may decrease while RAID scrubbing is in progress.

1. Go to **Main Menu > Storage & Snapshots**.
2. Click the **Global Settings** icon . The **Global Settings** menu opens.
3. Enable **RAID Scrubbing Schedule**.
4. Specify how often data scrubbing will run.
 - Daily
 - Weekly
 - Monthly
5. Specify when data scrubbing will run.



Tip

QNAP recommends specifying a time when the NAS is not in use, such as after business hours or on weekends.

6. Click **Apply**.

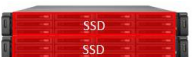
Data scrubbing will run according to the specified schedule. When data scrubbing is running on a RAID groups, the status of the group changes to *Scrubbing*.

Qtier

Qtier is a proprietary automated-tiering technology, designed to increase NAS storage performance and reduce the total cost of NAS ownership.

With Qtier, a storage pool can contain a mixture of solid-state drives (SSDs), hard disk drives (HDDs), and Serial Attached SCSI (SAS) drives. QTS creates a separate storage tier for each disk type, and then moves data between the tiers based on access frequency. Frequently accessed data is moved to the fastest disks for greater read and write performance. Infrequently accessed data is moved to the slower high-capacity disks for more cost effective data storage.

Qtier Benefits

	NAS Configuration	Cost	Storage Capacity	Read/Write Performance	Management Effort
	All HDDs	Low	High	Low	Low
	All SSDs	Very high	Low	High	Low

	NAS Configuration	Cost	Storage Capacity	Read/Write Performance	Management Effort
	SSDs and HDDs manually separated into two or more storage pools	Moderate	Medium	High for SSD pool, low for HDD pool	High (admin must manually move data between pools)
	Qtier with SSDs and HDDs in one Qtier-enabled storage pool	Moderate	Medium	High for frequently accessed data	Low (QTS automatically moves data between disks)

Qtier 2.0 IO Aware

Qtier 2.0 IO Aware is a feature available in QTS version 4.3.3 or later. With IO Aware, QTS reserves 25% of the SSD tier capacity in a Qtier storage pool for faster access performance. If data in the capacity or high speed tiers experiences a high number of read or write requests, QTS immediately moves it to reserved SSD space instead of waiting to move it using auto-tiering. This improves random I/O performance, similar performance as an SSD cache.

Qtier and SSD Cache Comparison



Note

Qtier can be used at the same time as SSD cache.

There are three main configuration options when configuring a NAS with a mixture of HDDs and SSDs.

Configuration	SSD Usage	HDD Usage
Qtier Storage Pool	Qtier Storage Pool (combined with HDDs)	Qtier Storage Pool (combined with SSDs)
SSD Cache	SSD cache	HDD-only storage pool
All-SSD Storage Pool	SSD-only storage pool	HDD-only storage pool

Qtier, SSD Cache, and All-SSD Storage Pool Comparison

	Qtier Storage Pool	SSD Cache	All-SSD Storage Pool
Total file storage space	High (SSDs + HDDs)	Moderate (HDDs only)	Low (SSDs only)
Maximum SSD capacity	No limit	Up to 4 TB depending on installed memory	No limit
SSD expansion	Expand as needed	Limited by available memory	Expand as needed
Applicable storage	Thick volumes, thin volumes and block-based LUNs in the pool	All volumes and LUNs on the NAS	Volumes and LUNs created on the SSDs
Data migration	Scheduled or when NAS load is low	Automatic	No migration required

	Qtier Storage Pool	SSD Cache	All-SSD Storage Pool
Data migration method	QTS writes incoming data to the SSD tier and moves data to different tiers based on access frequency.	- Write cache: QTS writes incoming data to the SSD cache and then flushes the cache to disk periodically. - Read cache: QTS copies data to the cache as it is accessed.	No migration required
Recommended use cases	- Total SSD capacity is high - I/O is predictable - The storage pool only occasionally experiences periods of intense random I/O access	- I/O is unpredictable and frequently happens in random bursts - Home usage, where the NAS will be used for a large range of different applications	Applications require consistent intensive random read-write access
Usage examples	File server, web server, email servers, basic database services (With Qtier IO Aware)	Video editing, virtualization	Business critical database or other application

Qtier Requirements

NAS Requirements

- The NAS must support Qtier. For a full list of compatible models, see <https://www.qnap.com/solution/qtier-auto-tiering>.
- The NAS should have at least 2 GB of installed memory. Using Qtier with less than 2 GB of memory may cause system instability.

Tier Requirements

A Qtier storage pool can have either two or three tiers.



Important

Each tier must have a total RAW storage capacity of at least 144 GB after configuring RAID.

Qtier Pool Configuration	Tier 1	Tier 2	Tier 3
Two tiers	Ultra-high speed	High speed OR capacity	N/A
Three tiers	Ultra-high speed	High speed	Capacity

Disk Requirements

Qtier Disk Types

Tier	Disk Type
Ultra-High Speed	• SATA 2.5" SSD • SAS 2.5" SSD • SATA M.2 SSD • PCIe/NVMe M.2 SSD
High Speed	• SAS HDD
Capacity	• SATA HDD • NL-SAS HDD

Qtier Creation

Creating a Qtier Storage Pool

For details on hardware and software requirements, see [Qtier Requirements](#).



Tip

Immediately after creating a Qtier storage pool, QTS starts moving data between tiers. This data migration may affect system storage performance. You should create the Qtier storage pool during a period of low NAS activity.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Perform one of the following actions.

Current state of the NAS	Action
No volumes or storage pools	Click New Storage Pool
One or more volumes or storage pools	Select Create > New Storage Pool

The **Create Storage Pool Wizard** opens.

3. Select **Enable Qtier (auto-tiering storage)**.
4. Click **Next**.
5. Create the ultra-high speed tier.
 - a. Click **SSD**.
 - b. Optional: Select an expansion unit.
 - c. Select one or more solid-state drives (SSDs).
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the ultra-high speed tier.
6. Optional: Create the high speed tier.
At least two different tiers are required in a Qtier storage pool.
 - a. Click **SAS**.

- b. Optional: Select an expansion unit.
 - c. Select one or more SAS hard disk drives (HDDs).
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the high speed tier.
7. Optional: Create the capacity tier.
At least two different tiers are required in a Qtier storage pool.
- a. Click .
 - b. Optional: Select an expansion unit.
 - c. Select one or more SATA or NL-SAS HDDs.
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the capacity tier.
8. Click **Next**.
9. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

10. Optional: Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
11. Click **Next**.
12. Verify the storage pool information.
13. Click **Create**.
A confirmation message appears.

**Warning**

All data on the selected disks will be deleted.

14. Click **OK**.

QTS creates the Qtier storage pool and starts moving data between tiers. QTS starts automatically tiering data after it has spent sufficient time analyzing data access patterns.

Enabling Qtier in an Existing Storage Pool

You can enable Qtier in an existing storage pool by adding different types of disk to the pool. For details on hardware and software requirements, see [Qtier Requirements](#).

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.

2. Select **Qtier > Upgrade with Qtier**.

The **Upgrade Pool to use Qtier Wizard** window opens.

3. Select a storage pool.

4. Click **Next**.

5. Create a second tier.

- a. Click ,  or .
- b. Select an expansion unit.
- c. Select one or more disks.
- d. Select a RAID type.
For details, see [RAID Types](#).
- e. Optional: Select the disk that will be used as a hot spare for the tier.

6. Optional: Create a third tier.

- a. Click ,  or .
- b. Optional: Select an expansion unit.
- c. Select one or more disks.
- d. Select a RAID type.
For details, see [RAID Types](#).
- e. Optional: Select the disk that will be used as a hot spare for the tier.

7. Click **Next**.

8. Optional: Configure SSD over-provisioning.

Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.



Tip

To determine the optimal amount of over-provisioning for your SSDs, download and run the SSD Profiling Tool app from App Center.

9. Click **Next**.

10. Verify the storage pool information.

11. Click **Finish**.

A confirmation message appears.



Warning

All data on the selected disks will be deleted.

12. Click **OK**.

The pool status changes to **Upgrading**. After Qtier is enabled, the pool status changes back to **Ready**.

Qtier Management

Storage Pool 1 Management

Qtier Auto Tiering

Storage Pool

Tiering Schedule

Tiering On Demand

Statistics

Qtier Auto-Tiering Status of Storage Pool 1

Tiering Status: Idle

Schedule Setting: Automatic data tiering

Detailed information of Storage Pool 1 (descending from highest to lowest)

Tier	Used	Total	Move Down	Move Up	Name/Alias	RAID Type
Tier1: Ultra-High Speed	33.2 %	204.59 GB	0 MB	--	RAID Group 1	RAID 0(2+0)
Tier2: High Speed	--	--	0 MB	0 MB	--	--
Tier3: Capacity	1.0 %	3.62 TB	--	0 MB	RAID Group 2	RAID 0(2+0)

Note: You still need proper spare disks and backup plan to protect tiered data.

Close

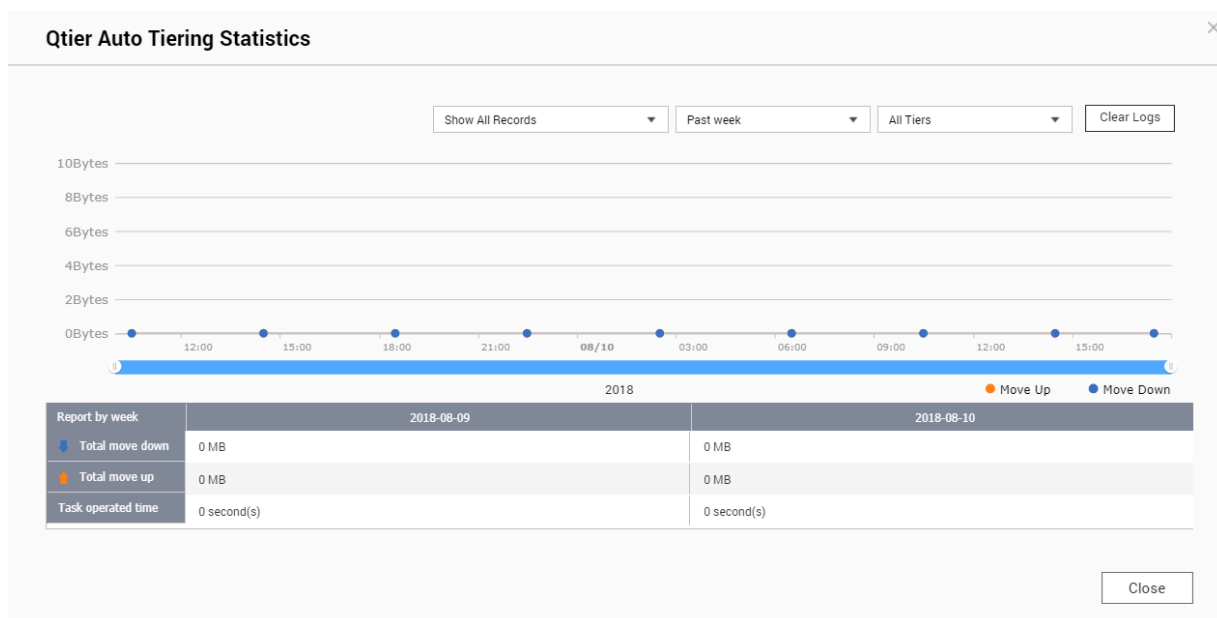
The Qtier Storage Pool Management Screen

Item	Description
Tiering Schedule	Select when QTS moves data between tiers. For details, see Configuring the Qtier Tiering Schedule .
Tiering on Demand	Select which LUNs and shared folders Qtier should perform auto tiering on. For details, see Configuring Tiering On Demand .
Statistics	View detailed on statistics on data movement between tiers. For details, see Qtier Statistics .
Tiering Status	The current status of Qtier. For details, see Qtier Status .
Schedule Setting	The current tiering schedule for this pool.
Tier	The tier name.
Used	Percentage of used space in the tier.
Total	Total storage capacity of the tier.
Move Down	The total amount of data moved to a slower tier.
Move Up	The total amount of data moved to a faster tier.
Name/Alias	The tier's RAID group.
RAID Type	The configuration of the tier's RAID group, including RAID type, number of disks and number of space disks.

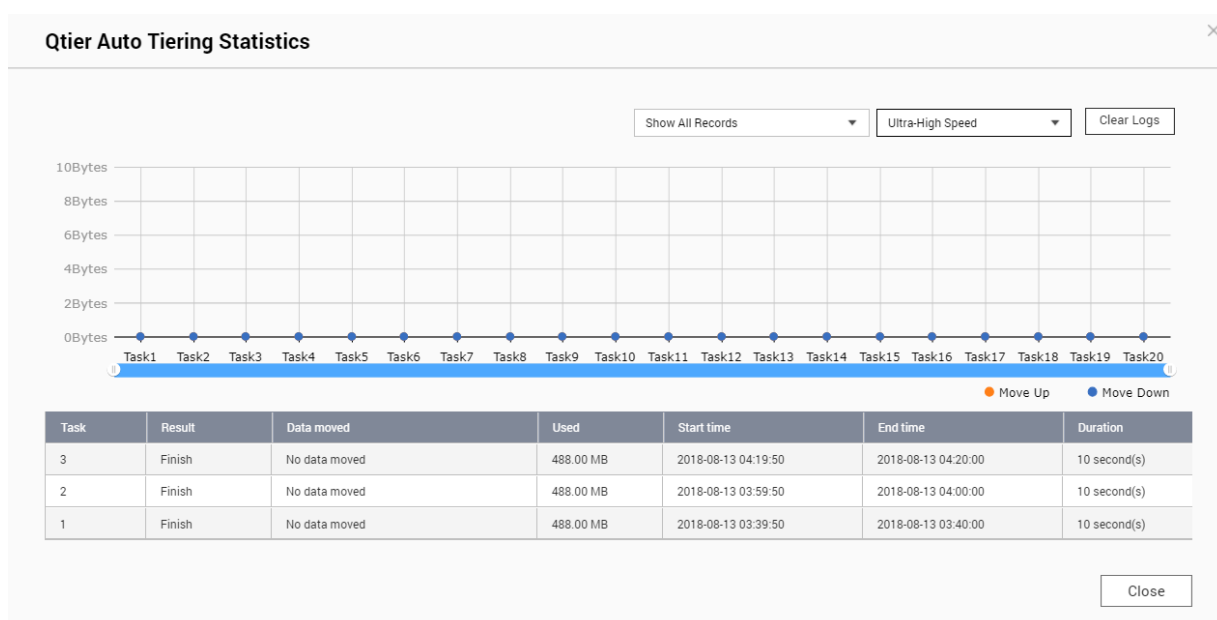
Qtier Statistics

The appearance and functionality of Qtier depends on the current tiering schedule.

Qtier Schedule	Qtier Statistics Screen Description
Automatic data tiering	Displays the total amount of data moved between tiers for the previous day, week, or month.
Manually set tiering schedule	Displays the total amount of data moved between tiers for the previous 20 scheduled tiering runs.



Qtier Statistics (Automatic data tiering)



Qtier Statistics (Manually set tiering schedule)

Qtier Status

Qtier Status Message	Description
Idle	Qtier is analyzing data access patterns but is not currently moving data
Processing	Qtier is moving data between tiers.
Canceling	A user stopped the tiering process.
Suspending	A user paused the tiering process.
Suspended	A user paused the tiering process. Qtier is inactive.
Resuming	A user resumed the tiering process from a paused state.
Resumed	Qtier is moving data between tiers. This is the same as <code>Processing</code> .

Qtier Tiering Schedule

Qtier can move data between tiers on a set schedule. NAS access speeds and system performance may decrease while Qtier is moving data.



Tip

Schedule Qtier to move data during periods of low usage, such as during the night or on weekends.

Configuring the Qtier Tiering Schedule

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a Qtier storage pool.
3. Click **Manage**.
The **Storage Pool Management** window opens.
4. Go to the **Qtier Auto Tiering** tab.
5. Click **Tiering Schedule**.
The **Qtier Auto Tiering Schedule Settings** window opens.
6. Select a schedule type.

Option	Description	Recommended usage	User Actions
Automatic data tiering	Qtier moves data whenever it detects that the Qtier storage pool is idle.	The NAS has no regular usage pattern. Data may be accessed at any time.	Select Enable exclusion schedule to specify times that Qtier should not perform data tiering.

Option	Description	Recommended usage	User Actions
Manually set tiering schedule	Qtier only move data at the times you specify.	The NAS has a regular known usage pattern. For example, if the NAS is primarily used in an office environment, Qtier can be scheduled to move data at night and on weekends.	Specify the hours on the calendar that Qtier should perform data tiering. You can configure the following settings: • Start minutes: Auto tiering will start at this number of minutes past the hour. • Run now: Start tiering data immediately.

7. Click **Apply**.

Tiering On Demand

Using Tiering On Demand, you can disable auto tiering for specific LUNs and shared folders in a Qtier storage pool. If auto tiering is disabled, QTS permanently moves all data in the LUN or folder to the slowest storage tier.



Important

You can only disable auto tiering for user data. Qtier always tiers system and application data stored in the pool.

Configuring Tiering On Demand

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a Qtier storage pool.
3. Click **Manage**.
The **Storage Pool Management** window opens.
4. Go to the **Qtier Auto Tiering** tab.
5. Click **Tiering On Demand**.
6. Configure auto tiering for each LUN and shared folder.
7. Click **Apply**.

Snapshots

A snapshot protects data by recording the state of a thick volume, thin volume, or LUN at a specific point in time. With snapshots, you can perform the following:

- Restore a volume or LUN to a previous state.
- Access and restore previous versions of files and folders.
- Create an identical copy of a volume or LUN.



Note

To use snapshots, your NAS model must support snapshots and have at least 1 GB of memory. For a list of compatible NAS models, see www.qnap.com/solution/snapshots.

Snapshot Storage Limitations

The maximum number of snapshots a NAS can store is determined by the NAS CPU manufacturer or NAS series, and installed memory.



Tip

For more information on NAS hardware specifications, go to <https://www.qnap.com>.

NAS CPU or Model	Installed Memory	Maximum Snapshots per NAS	Maximum Snapshots per Volume or LUN
- Intel CPU - AMD CPU	≥ 1 GB	32	16
	≥ 2 GB	64	32
	≥ 4 GB	1024	256
- Annapurna Labs CPU - TS-1635AX - TS-328 - TS-128A, TS-228A - TS-x51, TS-x51+	≥ 1 GB	32	16
	≥ 2 GB	64	32
	≥ 4 GB	256	64

Snapshot Creation

Taking a Snapshot

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a thick volume, thin volume, or block-based LUN.



Tip

To take a snapshot of a file-based LUN, take a snapshot of its parent volume.

3. Select **Snapshot > Take a Snapshot**.
A confirmation message appears.
4. Click **OK**.
The **Take a Snapshot** window opens.
5. Specify a name.
6. Specify a retention time.

Option	Description
Keep For	QTS retains the snapshot for the specified time period.
Keep this snapshot permanently	QTS retains the snapshot indefinitely, even when storage space is low.

7. Optional: Specify a description.
The description helps you to identify the snapshot.
8. Click **OK**.
A confirmation message appears.
9. Click **OK**.

QTS takes the snapshot. The snapshot appears in **Snapshot Manager**.

Configuring a Snapshot Schedule

Configure a snapshot schedule to take snapshots at regular intervals. Each volume and LUN can have a separate schedule.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a thick volume, thin volume, or LUN.
3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Click **Schedule Snapshot**.
The **Snapshot Settings** window opens.
5. Enable scheduling.
6. Specify the snapshot frequency.
7. Optional: Specify a retention time.
QTS retains the snapshot for the specified time period.
8. Optional: Enable smart snapshots.
When enabled, QTS only takes a snapshot if data on the volume or LUN was modified since the last snapshot was taken.
9. Optional: Specify a description.
The description helps you to identify the snapshot.
10. Click **OK**.
A confirmation message appears.
11. Click **OK**.

QTS starts taking snapshots according to the schedule.

Snapshot Management

Configuring Guaranteed Snapshot Space

Guaranteed snapshot space is storage pool space that is reserved for storing snapshots. Enabling this feature ensures that QTS always has sufficient space to store new snapshots.

Guaranteed Snapshot Space Status	Snapshot Storage Location
Disabled	Free space in the storage pool
Enabled	Guaranteed snapshot space until full, then free space in the storage pool

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a storage pool.
3. Select **Snapshot > Snapshot Manager** .
4. Select **Guaranteed Snapshot Space > Configure** .
5. Enable **Enable Guaranteed Snapshot Space**.
6. Select the amount of reserved space.

Option	Description
Recommended	Reserve a percentage of the total storage pool space.  Tip The default value is 20%.
Custom	Reserve a fixed amount of storage pool space.

7. Click **OK**.

Deleting Snapshots

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a thick volume, thin volume, or block-based LUN.
3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Optional: Change the view to list view.

- a. 

Click

- b. Select **List View**.

5. Select one or more snapshots.

6. 

Click

Snapshot Data Recovery

Restoring Files and Folders from a Snapshot



Tip

- Use snapshot revert to quickly restore all data on a volume or LUN. For details, see [Reverting a Volume](#).
- You can restore files and folders from a snapshots in File Station by enabling **Enable File Station Snapshot Directory for administrators**. For details, see [Snapshot Global Settings](#).

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .

2. Select a thick or thin volume.
The volume must contain at least one snapshot.
3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Select the files and folders to be restored.
6. Perform one of the following actions.

Action	Description
Select Restore > Restore Files	QTS restores the files and folders to their original locations on the volume or LUN.  Warning All changes made to files and folders after the snapshot was taken will be deleted.
Select Restore > Restore Files to	Restore the files and folders to a specified local folder or remote NAS. You can restore a single folder as a new shared folder.
In the menu bar, click 	Download the files and folders to your computer in a ZIP file.

QTS restores the files and folders then displays a confirmation message.

Reverting a Volume

Reverting restores a volume or LUN to the state at which the snapshot was taken. Restoring data using snapshot revert is significantly faster than restoring individual files and folders.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a thick or thin volume.



Important

The volume must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Revert Volume Snapshot**.



Warning

All changes made after the snapshot was taken will be deleted.

6. Optional: Select **Take a new snapshot before reverting**.
QTS takes a snapshot before starting the revert. This ensures that changes made on the volume or LUN are not permanently lost.
7. Click **Local Revert**.

The status of the volume changes to **Reverting**. QTS disables access to the volume until the revert process is finished.

Reverting a LUN

Reverting restores a volume or LUN to the state at which the snapshot was taken. Restoring data using snapshot revert is significantly faster than restoring individual files and folders.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a block-based LUN.



Important

The LUN must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Revert LUN Snapshot**.



Warning

All changes made after the snapshot was taken will be deleted.

6. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	QTS takes a snapshot before starting the revert. This ensures that changes made on the volume or LUN are not permanently lost.
Re-map LUN to the same iSCSI target after revert	If enabled, QTS automatically remaps the LUN to its current target after reverting. If disabled, you must manually remap the LUN after reverting.

7. Click **Local Revert**.

QTS unmaps the LUN from its iSCSI target. The status of the LUN changes to **Reverting**.

Restoring Files and Folders using Windows Previous Versions

- You must be using Windows 7, Windows 8 or Windows 10.
- The files must be stored on a thick volume, thin volume or LUN that has at least one snapshot.

QTS snapshots integrate with the Previous Versions feature, which enables Windows users to restore files and folders from a snapshot in Windows File Explorer.

1. In Windows, open a NAS shared folder using File Explorer.
For details on mapping a shared folder, see [Mapping a Shared Folder on a Windows Computer](#).
2. Right-click a file or folder, and then select **Properties > Previous Versions**.
A list of available previous versions appears. Each version corresponds to a snapshot containing the file or folder.
3. Select a previous version.

4. Select one of the following options.

Button	Description
Open	Open the previous version of the file or folder.
Restore	Overwrite the current version of the file or folder with the previous version.  Warning All changes made to the file or folder after the snapshot was taken will be deleted.

Snapshot Clone

Cloning creates a copy of a volume or LUN from a snapshot. The copy is stored in the same storage pool as the original volume or LUN.

Cloning a Volume

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a thick or thin volume.



Important

The volume must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Clone**.
The **Clone Snapshot** window opens.
6. Specify a volume alias.
7. Click **OK**.

QTS clones the volume and shared folders, and then displays a confirmation message.

Cloning a Block-Based LUN

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a block-based LUN.



Important

The LUN must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Clone**.
The **Clone Snapshot** window opens.

6. Specify a LUN name.
7. Optional: Select an iSCSI target.
QTS will map the LUN copy to the target.
8. Click **OK**.

QTS clones the LUN and then displays a confirmation message.

Snapshot Replica

Snapshot Replica is a snapshot-based full backup solution for QTS. With Snapshot Replica, you can back up a volume or block-based LUN to another storage pool, either on the same NAS or on a different QNAP NAS, using snapshots. Backing up data with Snapshot Replica reduces storage space and bandwidth requirements, and simplifies data recovery.

Protection Levels

Snapshot Replica can back up your snapshots to another storage pool on the local NAS, or to a remote NAS. These different backup configurations provide different levels of data protection.

Protects Against	Snapshots only	Snapshots + Local Snapshot Replica	Snapshots + Remote Snapshot Replica
Accidental modification or deletion of files	✓	✓	✓
Ransomware	✓	✓	✓
RAID Group Failure - Member disks fail - Member disks are removed from the NAS		✓	✓
Storage Pool Failure - One or more RAID groups in the pool fail - Pool is deleted		✓	✓
NAS Hardware Failure - NAS cannot power on - QTS encounters an error and cannot start - NAS is stolen			✓

Snapshot Replica Requirements

NAS	Requirement
Source and Destination NAS	Must be a QNAP NAS that supports snapshots.

NAS	Requirement
Source and Destination NAS	Must have at least 1GB of installed memory.
Source and Destination NAS	SSH port 22 and TCP data ports 50100-50199 must be open.
Destination NAS	The NAS must have at least one storage pool with free space greater than or equal to the size of the volume or LUN being backed up.
Destination NAS	Allow SSH connections must be enabled at Control Panel > Network & File Servers > Telnet / SSH .

Creating a Snapshot Replica Job



Important

When running a Snapshot Replica job for the first time, all data on the volume or LUN is transferred to the destination NAS. This may take a long time, depending on the network connection speed and the read/write speeds of both NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Snapshot Backup > Snapshot Replica**.
2. Click **Create a Replication Job**.
The **Create a Snapshot Replication Job** wizard opens.
3. Select the source volume or LUN.
4. Optional: Specify a job name.



Tip

The default job name is the first 6 characters of the source volume or LUN name followed by "_rep".

5. Click **Next**.
6. Specify the IP address of the destination NAS.
Perform one of the following actions.

Action	Destination NAS Location	Description
Manually specify the NAS address	LAN, WAN, Internet	You can enter an IP address, hostname, or FQDN.
Click Detect and then select a NAS from the list	LAN	QTS displays a list of all QNAP NAS devices on the local network. You can sort the list by hostname or IP address.
Click Local Host	N/A	Choose this option to replicate snapshots between different storage pools on the same NAS.

7. Enter the password for the default admin account on the destination NAS.
8. Optional: Specify a port.



Tip

The default port is 22.

9. Click **Test.**

QTS connects to the destination NAS using the specified admin password, and then checks that there is sufficient space at the destination to store the source volume or LUN.

10. Click **Next.****11. Specify how many replicated snapshots will be kept on the destination NAS.**

After the specified number is reached, the QTS will delete the oldest snapshot each time it replicates a new snapshot.

12. Select the destination storage pool.**13. Select a backup plan.**

Backup Plan	Description
Start replication job after taking a local snapshot	The replica job will run each time QTS creates the specified number of snapshots. These snapshots may be created manually or on a schedule.
Start replication job on a schedule	The replica job replicates all snapshots created since it was last run. If no new snapshots were created, it will not replicate any data. Choose one of the following scheduling options: - Run on a schedule: The job automatically runs daily, weekly, or monthly. Settings: - Schedule: How often the job runs - Day: The day that the job runs on - Expiration date: The replica job stops running after this date - Frequency: How often the job runs on the days specified by "Schedule" and "Day" - Start at: The time that the job starts running. - Run once: The job runs once on a specific time and day. - Manually start: The job does not run unless a user starts it.
Take a new snapshot on a schedule, then run replication job	The job runs daily, weekly, or monthly. QTS takes a new snapshot immediately before starting the job. This ensures that there is always at least one snapshot to replicate.

14. Click **Next.****15. Optional: Configure transfer settings.**

Setting	Description
Encrypt transfer	QTS encrypts the snapshot before sending it. - The job must be run by the NAS admin user - The port used by this job must be the same as the SSH port on the destination NAS
Compress transfer	QTS will compress snapshots when replicating them. This consumes more CPU and system memory, but reduces the amount of bandwidth required.  Tip Enable this setting in low bandwidth networks, or if the NAS devices are connected through a WAN.
Maximum transfer speed	Limit how much network bandwidth this job uses.

- Export the source data to an external storage device.
To save time and bandwidth, you can export the source data to a connected external storage device such as a USB disk. After connecting the external storage device to the destination NAS, QTS will import the source data when the job is next run.
- Click **Next**.
- Optional: Select **Execute backup immediately**.
When enabled, the job will run immediately after being created.
- Review the job information.
- Click **Finish**.

Snapshot Replica Management

To manage snapshot replica setting and jobs, go to **Main Menu > Storage & Snapshots > Snapshot Backup > Snapshot Replica**.

Overview

Storage

Snapshot

Storage

Disks/VJBOD

Storage/Snapshots

Cache Acceleration

External Storage

Snapshot Backup

Snapshot Replica

Snapshot Vault

iSCSI

iSCSI Storage

Remote Disk

LUN Import/Export

Snapshot Replica:

Create a Replication Job

Options

Storage Pool 1

Storage Pool 2

Partial Protection

Volumes/LUNs - Total: 7, Protected by Snapshots: 2, Protected by Snapshot Replica: 1

DataVol1 (Thick volume) 0 Local Snapshot

There are no snapshot replica jobs yet.

DataVol1_1 (Thick volume) 0 Local Snapshot

There are no snapshot replica jobs yet.

BackupVolume1 (Thick volume) 2 Local Snapshot

There are no snapshot replica jobs yet.

BackupVolume2 (Thick volume) 4 Local Snapshot

Success: BackupVolu_rep Last Finished: 2018/9/21

2018/09/20 Earliest

2018/09/20 Latest

2018/09/21 Now

Remote Snapshots: 4

Storage locations: 2

Job List

Replica Job	Destination	Schedule	Last Finish / Next Start	Progress	Action
BackupVolu_rep	Ripple431 P2 172.17.31.240 4	☒ Daily, Once a day, 00:00	2018/9/21 00:00:29 2018/9/22 00:00:00	Finished	
BackupVolu_rep1	TW-TEST4 172.17.49.153 4	☐ Not scheduled	2018/9/20 19:11:57 -	Finished	

Snapshot Replica Job Actions

Icon	Description
	Enable or disable the schedule
	Start
	Stop
	Edit settings
	View logs
	Delete

Snapshot Replica Options

Setting	Description	Default Value
Timeout (seconds)	When a job is interrupted, QTS waits the specified number of seconds before canceling the job and marking it as failed.	600
Number of retries	When a job fails, QTS runs the job again the specified number of times.	3

Data Recovery on a Source NAS

Restoring Files and Folders from a Remote Snapshot



Important

Restoration time depends on the amount of data being restored and the connection speed between the two NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a thick or thin volume.



Important

The volume must contain at least one snapshot.

3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Select the files and folders to be restored.
7. Perform one of the following actions.

Action	Description
Select Restore > Restore Files	QTS restores the files and folders to their original locations on the volume or LUN.  Warning All changes made to files and folders after the snapshot was taken will be deleted.
Select Restore > Restore Files to	Restore the files and folders to a specified local folder or remote NAS. You can restore a single folder as a new shared folder.
In the menu bar, click 	Download the files and folders to your computer in a ZIP file.

QTS restores the files and folders then displays a confirmation message.

Reverting a Volume Using a Remote Snapshot

Reverting restores a volume or LUN to the state at which the snapshot was taken. Restoring data using snapshot revert is significantly faster than restoring individual files and folders.



Important

Restoration time depends on the amount of data being restored and the connection speed between the two NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a thick or thin volume.



Important

The volume must have at least one snapshot on a remote NAS.

3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Click **Revert Volume Snapshot**.



Warning

All changes made after the snapshot was taken will be deleted.

7. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	QTS takes a snapshot before starting the revert. This ensures that changes made on the volume or LUN are not permanently lost.
Enable encryption during transfer	QTS encrypts the snapshot before sending it for additional security.

**Warning**

If the network connection is interrupted or if the storage configuration of the source or destination NAS changes while reverting, the volume might become inaccessible. If this happens, revert the volume again using a local or remote snapshot.

8. Click **Revert Volume Snapshot**.
The **Remote Revert Warning** window opens.
9. Enter the QTS administrator password.
10. Click **OK**.

The status of the volume changes to `Remote Reverting`. QTS disables access to the volume until the revert process is finished.

Reverting a LUN Using a Remote Snapshot

Reverting restores a volume or LUN to the state at which the snapshot was taken. Restoring data using snapshot revert is significantly faster than restoring individual files and folders.

**Warning**

- While reverting, ensure that data is not being accessed on the LUN. The safest way to do this is to disconnect all iSCSI initiators. Accessing the LUN during a snapshot revert might result in data loss.
- Restoration time depends on the amount of data being restored and the connection speed between the two NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a block-based LUN.

**Important**

The LUN must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Click **Revert LUN Snapshot**.

**Warning**

All changes made after the snapshot was taken will be deleted.

7. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	QTS takes a snapshot before starting the revert. This ensures that changes made on the volume or LUN are not permanently lost.
Enable encryption during transfer	QTS encrypts the snapshot before sending it for additional security.

Setting	Description
Re-map LUN to the same iSCSI target after revert	If enabled, QTS automatically remaps the LUN to its current target after reverting. If disabled, you must manually remap the LUN after reverting.

**Warning**

If the network connection is interrupted or if the storage configuration of the source or destination NAS changes while reverting, the LUN might become inaccessible. If this happens, revert the volume again using a local or remote snapshot.

8. Click **Remote Revert**.
The **Remote Revert Warning** window opens.
9. Enter the QTS administrator password.
10. Click **OK**.

QTS unmaps the LUN from its iSCSI target. The status of the LUN changes to *Reverting*.

Cloning a Volume from a Remote Snapshot

**Important**

The time required to clone the volume depends on the amount of data stored on the volume and the connection speed between the two NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a thick or thin volume.

**Important**

The volume must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Click **Clone**.
The **Clone Snapshot** window opens.
7. Specify a volume alias.
8. Select a storage pool.
9. Select **Enable encryption during transfer**.
QTS encrypts the snapshot before sending it for additional security.
10. Click **OK**.

QTS clones the volume and shared folders, and then displays a confirmation message.

Cloning a Block-Based LUN from a Remote Snapshot

1. Go to **Main Menu > Storage & Snapshots > Storage > Storage/Snapshots**.
2. Select a block-based LUN.



Important

The LUN must have at least one snapshot.

3. Select **Snapshot > Snapshot Manager** .
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Click **Clone**.
The **Clone Snapshot** window opens.
7. Specify a LUN name.
8. Select a storage pool.
9. Optional: Select an iSCSI target.
QTS will map the LUN copy to the target.
10. Select **Enable encryption during transfer**.
QTS encrypts the snapshot before sending it for additional security.
11. Click **OK**.

QTS clones the LUN and then displays a confirmation message.

Data Recovery on a Destination NAS

Snapshot Vault

After setting a NAS as the destination for a Snapshot Replica job, the replicated snapshots are stored in Snapshot Vault. Each replica job has its own separate vault.

Overview

Storage

Snapshot

Storage

Disks/VJBOD

Storage/Snapshots

Cache Acceleration

External Storage

Snapshot Backup

Snapshot Replica

Snapshot Vault

iSCSI

iSCSI Storage

Remote Disk

LUN Backup

Snapshot Vault:

Snapshot Vault is the backup center for storing and managing all of the snapshots created remotely from another NAS.

Storage Pool 1

Storage Pool 1 Snapshot Vault

Total - Snapshot Vault: 3

Storage Pool 1			Source			Action
Vault Name	Snapshot	Total Size	Job Name/Schedule	Source	Last finish time:	Action
✓ V_BackupVol_	Ready Snapshots: 1	9.28 GB	BackupVolu_rep (Stopped) Start replication job after takin...	TW-TEST3 172.17.48.56	2018/9/19 17:26:42	
✓ V_BackupVol_	Ready Snapshots: 2	1.41 GB	BackupVol_rep1 (Finished) Not scheduled	TW-TEST3 172.17.49.152	2018/9/20 19:10:49	
✓ V_DataVol2	Ready Snapshots: 2	1.41 GB	DataVol2_rep (Finished) Start replication job after takin...	TW-TEST4 Local Host	2018/5/18 17:29:07	

Restoring Files and Folders from a Snapshot Vault

1. Go to **Main Menu > Storage & Snapshots > Snapshot Backup > Snapshot Vault** .

2. Select a storage pool.
3. On a vault, click . The **Snapshot Vault** window opens.
4. Optional: Unlock the vault.
If the original source volume is encrypted, you must unlock the vault with the encryption password.
 - a. Click **Unlock**.
 - b. Enter the encryption password or upload the encryption key.
 - c. Click **OK**.
5. Select a snapshot.
6. Select the files and folders to be restored.
7. Click **Restore Files To**.
8. Specify a restore location.
9. Click **OK**.

Cloning a Volume from a Snapshot Vault

1. Go to **Main Menu > Storage & Snapshots > Snapshot Backup > Snapshot Vault**.
2. Select a storage pool.
3. On a vault, click . The **Snapshot Vault** window opens.
4. Optional: Unlock the vault.
If the original source volume is encrypted, you must unlock the vault with the encryption password.
 - a. Click **Unlock**.
 - b. Enter the encryption password or upload the encryption key.
 - c. Click **OK**.
5. Select a snapshot.
6. Click **Clone**.
The **Clone Snapshot** window opens.
7. Specify a volume alias.
8. Click **OK**.

QTS clones the volume and shared folders, and then displays a confirmation message.

Cloning a Block-Based LUN from a Snapshot Vault



Important

The time required to create the LUN depends on the amount of data stored on the LUN and the connection speed between the two NAS devices.

1. Go to **Main Menu > Storage & Snapshots > Snapshot Backup > Snapshot Vault** .
2. Select a storage pool.
3. On a vault, click  .
The **Snapshot Vault** window opens.
4. Optional: Unlock the vault.
If the original source volume is encrypted, you must unlock the vault with the encryption password.
 - a. Click **Unlock**.
 - b. Enter the encryption password or upload the encryption key.
 - c. Click **OK**.
5. Select a snapshot.
6. Click **Clone**.
The **Clone Snapshot** window opens.
7. Specify a LUN name.
8. Optional: Select an iSCSI target.
QTS will map the LUN copy to the target.
9. Click **OK**.

QTS clones the LUN and then displays a confirmation message.

4. System Settings

General Settings

Settings	Description
System Administration	This screen allows you to specify the server name and ports and configure secure connection settings.
Time	Time settings affect event logs and scheduled tasks. This screen allows you to specify the time zone and format and configure the system date and time.
Daylight Saving Time (DST)	Daylight saving time (DST) settings apply only to regions that use DST. This screen allows you to either automatically adjust the system clock or manually configure the settings.
Codepage	This screen allows you to select the language that the NAS uses to display file and directory information.
Region	This screen allows you to select a region for your NAS. System and application content and services are localized according to the selected region.
Login Screen	This screen allows you to customize the NAS login screen.

Configuring System Administration Settings

1. Go to **Control Panel > System > General Settings > System Administration**.
2. Specify the following information.

Field	User Action
Server name	Specify a name containing up to 14 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9  Important The server name cannot consist of numbers only. • Dashes (-)  Important Ensure that dashes are not preceeded or followed by a space.
System port	Specify the port that you will use to access the web interface. The default port is 8080.
Disable and hide multimedia functions	This option is disabled by default.  Important Disabling this option will make multimedia apps (e.g., Photo Station, Music Station, Download Station) and services (e.g., Media Library, DLNA server, iTunes server) unusable.

Field	User Action
Enable secure connection (HTTPS)	Select this option and specify a port number to allow users to connect to the NAS using HTTPS.
Force secure connection (HTTPS) only	Select this option to require all users to connect to the NAS using only HTTPS.
Do not allow QTS embedding in IFrames	- Select this option to prevent websites from embedding QTS using IFrames. - Optional: Select Allow only specific websites to embed QTS in IFrames. - Click Allowed Websites. The Allowed Websites window appears. - Optional: Click Add to add a website to the list. The Add Host Name window appears. - Specify a host name. - Click Add. The host name is added to the allowed websites list. - Optional: Select a website, and then click Delete to delete a website from the list. - Click Apply.

3. Click **Apply**.

Configuring Time Settings



Important

You must configure the system time correctly to avoid the following issues.

- When using a web browser to connect to the NAS or save a file, the displayed time of the action is incorrect.
- Event logs do not reflect the exact time that events occurred.
- Scheduled tasks run at the wrong time.

1. Go to **Control Panel > System > General Settings > Time**.
2. Select a time zone.
3. Specify the date and time format.
4. Select the time setting.

Option	User Action
Manual setting	Specify the date and time.

Option	User Action
Synchronize with an Internet time server automatically	Ensure that your NAS is connected to the Internet, and then specify the following information: • Server: Name of the Network Time Protocol (NTP) server Examples: time.nist.gov, time.windows.com • Time interval: Number of hours or days between each time synchronization task
Set the server time the same as your computer time	Click Update .

5. Click **Apply**.

Configuring Daylight Saving Time

These settings are available for NAS users in regions that use Daylight Saving Time (DST). Users outside these regions can disregard these settings.

1. Go to **Control Panel > System > General Settings > Daylight Saving Time**.
2. Select **Adjust system clock automatically for daylight saving time**.
3. Optional: Select **Enable customized daylight saving time table**.
4. Optional: Perform any of the following actions.

Action	Steps
Add DST data	a. Click Add Daylight Saving Time Data. The Add Daylight Saving Time Data window appears. b. Specify a time period and the number of minutes to offset. c. Click Apply.
Edit DST data	a. Select a DST schedule from the table. b. Click . c. Specify a time period and the number of minutes to offset. d. Click Apply.
Delete DST data	a. Select a DST schedule from the table. b. Click Delete. c. Click OK.

5. Optional: Select a DST schedule from the table.
6. Click **Apply**.

Configuring Codepage Settings

All files and directories on the NAS use Unicode encoding. If your operating system or FTP client does not support Unicode, you must configure the following settings to properly view files and directories on the NAS.

1. Go to **Control Panel > System > General Settings > Codepage** .
2. Select the language of your operating system.
3. Click **Apply**.

Configuring Region Settings



Important

The NAS region settings affect device connectivity and the functionality, content, and validity of some applications, utilities, licenses, and certificates. Ensure that you select the correct region to avoid errors.

1. Go to **Control Panel > System > General Settings > Region** .
2. Select a region.

Region	Description
Global	Select this region if the NAS is located outside of China.
China	Select this region if the NAS is located in China.

3. Click **Apply**.

Configuring the Login Screen

1. Go to **Control Panel > System > General Settings > Login Screen** .
2. Configure the following settings.

Field	User Action
Show firmware version	Select this option to display the QTS firmware version.
Show the link bar	Select this option to display links to myQNAPCloud, QNAP Utilities, and Feedback.
Background	Select a background image or fill color.
Logo	Select a logo.
Message	Specify a message that will appear on the login screen. You can enter a maximum of 120 ASCII characters. You can also select the font color and size.

3. Click **Preview** to view the changes.
4. Click **Apply**.

Security

Configuring the Allow/Deny List

1. Go to **Control Panel > System > Security > Allow/Deny List** .
2. Select an option.

Option	Description	User Action
Allow all connections	The NAS can connect to all IP addresses and network domains.	Select Allow all connections .
Use IP deny list	The NAS cannot connect to any IP address or network domains included the IP deny list.	a. Select Deny connections from the list. b. Click Add. The IP configuration window appears. c. Specify an IP address, netmask, or IP range. d. Click Create.  Tip To remove an IP address, netmask, or IP range, select an entry from the table, and then click Remove.
Use IP allow list	The NAS can only connect to the IP addresses or network domains included on the IP allow list.	a. Select Allow connections from the list only. b. Click Add. The IP configuration window appears. c. Specify an IP address, netmask, or IP range. d. Click Create.  Tip To remove an IP address, netmask, or IP range, select an entry from the table, and then click Remove.

3. Click **Apply**.

Configuring Network Access Protection

- Go to **Control Panel > System > Security > Network Access Protection**.
- Select **Enable Network Access Protection**.
- Select the connection methods you want to protect.
- Optional: Specify the following information.
 - Time period
 - Maximum number of unsuccessful login attempts within the time period
 - Amount of time the IP will be blocked
- Click **Apply**.

Certificate & Private Key

Secure Sockets Layer (SSL) is a protocol used for secure data transfers and encrypted communication between web servers and browsers. To avoid receiving alerts or error messages when accessing the web interface, upload an SSL certificate from a trusted provider.

Replacing the SSL Certificate and Private Key



Warning

The NAS supports only X.509 PEM certificates and private keys. Uploading an invalid security certificate may prevent you from logging in to the NAS through SSL. To resolve the issue, you must restore the default security certificate and private key.

For details, see [Restoring the Default SSL Certificate and Private Key](#).

1. Go to **Control Panel > System > Security > Certificate & Private Key**.
2. Click **Replace Certificate**.
The **Replace Certificate** window appears.
3. Select an option.

Option	Description
Import certificate	This option allows you to import an SSL certificate and private key from your computer.
Get from Let's Encrypt	This option uses the Let's Encrypt service to validate and issue a certificate for your specified domain.
Create self-signed certificate	This option allows you to create a self-signed certificate.

4. Click **Next**.
A configuration window appears.
5. Perform any of the following actions.

Option	User Action
Import certificate	a. Click Browse to upload a valid certificate and private key. b. Optional: Click Browse to upload an intermediate certificate.
Get from Let's Encrypt	a. Specify a domain name containing a maximum of 63 ASCII characters, without spaces. b. Specify a valid email address. c. Optional: Specify an alternative name.  Tip Use "," to separate multiple aliases. Example: 123.web.com, 789.web.com

Option	User Action
Create self-signed certificate	Configure the following information. • Private key length • Common name • Email • Country • State/Province/Region • City • Organization • Department

6. Click **Apply**.

Downloading the SSL Certificate and Private Key

1. Go to **Control Panel > System > Security > Certificate & Private Key** .
2. Click **Download Certificate**.
A dialog box appears.
3. Select **Certificate**, **Private Key**, or both.
4. Click **OK**.
QTS downloads the selected files to your computer.

Restoring the Default SSL Certificate and Private Key

1. Go to **Control Panel > System > Security > Certificate & Private Key** .
2. Click **Restore to Default**.
A confirmation message appears.
3. Click **OK**.

Configuring the Password Policy

1. Go to **Control Panel > System > Security > Password Policy** .
2. Under **Password Strength**, select the criteria.
 - A new password has to contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
 - No character in the new password may be repeated three (or more) times consecutively.
Example: AAA.
 - The password must not be the same as the associated username, or the username reversed.
Example: Username: user1, password: 1resu.
3. Under, **Change Password**, select **Force NAS user to regularly change their password**.



Important

Enabling this setting disables the **Disallow the user to change password** setting.

- a. Specify the maximum number of days that the password is valid.
- b. Optional: Select **Send a notification email to users a week in advance of their password expiring**.

4. Click **Apply**.

Hardware

Configuring General Hardware Settings

1. Go to **Control Panel > System > Hardware > General**.
2. Configure the following settings.

Settings	User Action
Enable configuration reset switch	Select this option to enable the reset button. For details on the reset button, see System Reset and Restore to Factory Default .
Enable disk standby mode	Select this option to allow the NAS drives to enter standby mode if there is no disk access within the specified period. Disk status LED remains on during standby mode.
Enable light signal alert	Select this option to allow the status LED to flash when free space on the NAS is less than the set value.  Note Select this option only for legacy volumes. For details, see Legacy Volumes.
Enable write cache (EXT4 delay allocation)	If the NAS disk volume uses EXT4, select this option for higher write performance. If the NAS is set as a shared storage in a virtualized or clustered environment, disable this option.  Warning When this option is enabled, an unexpected system shutdown may lead to data loss.
Enable warning alert for redundant power supply on the web-based interface	If two power supply units (PSU) are installed on the NAS and connected to power sockets, select this option to receive warnings for the PSUs. The NAS will trigger an audio alert and record error messages in System Logs if a PSU is unplugged or not responding correctly. If only one PSU is installed on the NAS, do not select this option.  Note This function is only applicable for some models.
Run user-defined processes during startup	Select this option to run user-defined processes during startup.

Settings	User Action
Turn on LED	Select this option to turn on the LED, set its brightness level, and set a schedule for brightness setting.  Note This function is only applicable for some models.

3. Click **Apply**.

Configuring Audio Alert Settings

1. Go to **Control Panel > System > Hardware > Audio Alert**.
2. Configure any of the following settings.

Setting	Description
System operations	Select this option to trigger an audio alert every time the NAS starts, shuts down, or upgrades firmware.
System events	Select this option to trigger an audio alert when errors or warnings occur.
Enable speech notification	Select this option to replace some audio alerts with speech. You can select a language and modify the volume.  Tip Click Test to check the modified speech settings. If there is no sound, another app may be using the speaker.

3. Click **Apply**.

Configuring Smart Fan Settings

1. Go to **Control Panel > System > Hardware > Smart Fan**.
2. Select fan rotation speed settings.



Note

Some NAS models allow users to separately adjust system and CPU smart fans.

Setting	User Action
Enable Smart Fan (recommended)	Select from the two automatic fan speed adjustment options. - QTS monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. - QTS adjusts the fan speed according to user-specified temperatures.  Note Modes are only available for system fans. Quiet mode: Fans run on low speed to decrease noise. Normal mode: Fans run on normal speed. This is the default setting. Performance mode: Fans run on high speed to lower the system temperature. This mode is suitable for high loading systems.
Set fan rotation speed manually	Move the slider to set the fan speed.

- Click **Apply**.

Backup Battery Unit (BBU)

You can schedule a learning cycle for the backup battery units (BBUs). A learning cycle is when a controller performs a battery calibration operation to determine the battery's condition. During this cycle, the system switches to write-through mode to protect data integrity.

In write-through mode, the NAS writes data directly to HDDs/SSDs instead of writing to the RAM first. This prevents data loss if a power outage occurs before the NAS finishes writing data.

This function is only available for models with redundant power supply units.

Configuring the Backup Battery Unit (BBU) Settings



Important

QNAP strongly recommends scheduling the learning cycle during off-peak hours.

- Go to **Control Panel > System > Hardware > BBU**.
- Select **Enable BBU learning schedule**.
- Specify a learning cycle schedule.
- Click **Apply All**.

Configuring Graphics Card Settings

- Go to **Control Panel > System > Hardware > Graphics Card**.
QTS lists the available graphics cards.
- Identify the graphics cards you want to configure.
- Under **Resource Use**, select an OS or an application.

**Note**

Some functions are only applicable for certain models and graphics cards.

OS or Application	Description
QTS	QTS applications share graphics card resources for transcoding. - Select Hardware Transcoding to allow QTS software to use graphics card resources to speed up transcoding tasks. Only one card can be assigned to hardware transcoding. - Select Output to use graphics card resources for video output of HD Station or Linux Station. Only one card can be assigned to output.
Virtualization Station	Virtualization Station has exclusive use of all graphics card resources.
Container Station	Container Station has exclusive use of all graphics card resources.

- Click **Apply**.

Power

You can configure Wake-on-LAN (WOL), select a NAS behavior after power outage, and specify power schedules.

EuP Mode

Energy-using Products (EuP) is a directive designed to improve energy efficiency of electrical devices, reduce use of hazardous substances, and improve environment-friendliness of the product.

Configuring EuP Mode

- Go to **Control Panel > System > Power > EuP Mode Configuration**.
- Select a mode.

Mode	Description
Enable	When enabled, Wake-on-LAN, power recovery, and power schedule settings are disabled. The NAS keeps power consumption below 1W when powered off.
Disable	When disabled, power consumption of the NAS is slightly higher than 1W when powered off. EuP mode is disabled by default.

- Click **Apply**.

Wake-on-LAN (WOL)

You can power on the NAS remotely using the Wake-on-LAN (WOL) protocol in Qfinder. This feature is enabled by default.

**Important**

If the power cable is disconnected when the NAS is powered off, WOL will not work until the NAS has been manually powered on.

Enabling or Disabling Wake-on-LAN (WOL)

1. Go to **Control Panel > System > Power > Wake-on-LAN (WOL)** .
2. Select **Enable** or **Disable**.
3. Click **Apply**.

Power Recovery

This feature allows you to configure the power on and off status of the NAS after a power outage.

Configuring the Power Recovery Settings

1. Go to **Control Panel > System > Power > Power Recovery** .
2. Select a power recovery setting.
 - Restore the previous NAS power state.
 - Turn on the NAS automatically.
 - Keep the NAS turned off.
3. Click **Apply**.

Power Schedule

This feature allows you to schedule automatic system power on, power off, and restarts at specified times.

Configuring the Power Schedule

1. Go to **Control Panel > System > Power > Power Schedule** .
2. Select **Enable schedule**.
3. Perform any of the following tasks.

Task	User Action
Add a scheduled action.	 Note One schedule is shown by default. a. Click Add. b. Select the following. • Action: Select whether you want to shut down, restart, or turn on the NAS. • Schedule Type: Select the frequency of the action. • Hour and Minute: Select the time of day to perform the action.

Task	User Action
Remove a scheduled action.	Click Remove .  Note Schedules are removed starting from the bottom.

- Optional: Select **Postpone scheduled restart/shutdown when a replication job is in progress**.
- Click **Apply**.

Firmware Update

QNAP recommends keeping your QTS version up to date. This ensures that your NAS can benefit from new features, enhancements, and bug fixes.

Checking for Live Updates

- Go to **Control Panel > System > Firmware Update > Live Update**.
- Click **Check for Update**.
QTS checks for available firmware updates. You can choose to update QTS if there is an available update.
- Optional: Select one or more of the following options.
 - Automatically check if a newer version is available when logging into the NAS web administration interface.
 - Join the QTS Beta program to receive beta update notifications.



Note

Joining the QTS Beta program allows you to use the latest QTS features and applications before they are officially released.

- Click **Apply**.

Updating the Firmware Manually



Important

- QNAP recommends backing up all data on the NAS before updating QTS.
- The update may require several minutes or longer, depending on your hardware configuration and network connection. Do not power off the NAS during the update.

- Download the NAS firmware.
 - Go to <http://www.qnap.com/download>.
 - Select the number of drive bays on your NAS model.
 - Select your NAS model.
 - Read the release notes and confirm the following:
 - The NAS model matches the firmware version.

- Updating the firmware is necessary.
 - e. Ensure that the product model and firmware version are correct.
 - f. Download the firmware package.
 - g. Extract the firmware image file.
2. Go to **Control Panel > System > Firmware Update > Firmware Update**.
 3. Click **Browse** and then select the extracted firmware image file.
 4. Click **Update System**.

Updating the Firmware Using Qfinder Pro



Important

- QNAP recommends backing up all data on the NAS before updating QTS.
- The update may require several minutes or longer, depending on your hardware configuration and network connection. Do not power off the NAS during the update.

1. Download the NAS firmware.
 - a. Go to <http://www.qnap.com/download>.
 - b. Select the number of drive bays on your NAS model.
 - c. Select your NAS model.
 - d. Read the release notes and confirm the following:
 - The NAS model matches the firmware version.
 - Updating the firmware is necessary.
 - e. Ensure that the product model and firmware version are correct.
 - f. Download the firmware package.
 - g. Extract the firmware image file.
2. Open Qfinder Pro.
Qfinder Pro displays a list of NAS devices on your network.
3. Select a NAS model from the device list.
4. Go to **Tools > Update Firmware**.



Tip

You can also right-click the NAS model on the list and then select **Update Firmware**.

The **Firmware Update** window appears.

5. Specify your QTS username and password.
To update the firmware, you must be the administrator of the selected NAS.
Qfinder Pro displays the **Update Firmware** screen.
6. Click **Browse** and then select a firmware image file.

7. Perform one of the following actions:

Action	Steps
Update a single NAS device	Select the NAS that you want to update.
Update multiple NAS devices of the same model	- Select a NAS model from the list. - Select Update all the devices with the same model number within the network. - Select the NAS devices that you want to update.

8. Click **Start**.

Backup/Restore

QTS provides system backup and restore features to help protect your data in the event of data loss or system failure.

Backing Up System Settings

- Go to **Control Panel > System > Backup/Restore > Backup/Restore Settings**.
- Click **Backup**.

QTS exports the system settings as a BIN file and downloads the file to your computer.

Restoring System Settings



Warning

If the selected backup file contains user or user group information that already exists on the NAS, QTS will overwrite the duplicate information.

- Go to **Control Panel > System > Backup/Restore > Backup/Restore Settings**.
- Click **Browse**.
- Select a valid BIN file that contains the QTS system settings.
- Click **Restore**.

System Reset and Restore to Factory Default

QTS provides several options for resetting or restoring the NAS to its default state.



Important

QNAP recommends backing up your data before performing this task.

Option	Description	Steps
Basic system reset	This resets the following settings to the default values without deleting the user data stored on the disks. • System administrator password: admin • TCP/IP configuration: • Obtain IP address settings automatically via DHCP • Disable jumbo frames • System port: 8080 (system service port) • Security level: Low (Allow all connections) • LCD panel password: (blank) • VLAN: Disabled • Service binding: All NAS services can run on all available network interfaces.	1. Power on the NAS. 2. Press and hold the reset button for 3 seconds.
Advanced system reset	This performs a basic system reset and then restores the QTS default settings, deleting all users, user groups, and shared folders previously created. The user data stored on the disks is retained.  Note To retrieve old data after an advanced system reset, re-create the previous folder structure on the NAS.	Perform an advanced system reset using one of the following methods. • Using QTS: a. Go to Control Panel > System > Backup/Restore > Restore to Factory Default. b. Click Reset Settings. c. Choose to restart or shut down the NAS after the system is reset. d. Click OK. • Using the reset button: a. Power on the NAS. b. Press and hold the reset button for 10 seconds.

Option	Description	Steps
Restore factory default settings and format all volumes	This restores the default system settings and formats all disk volumes.	1. Go to Control Panel > System > Backup/Restore > Restore to Factory Default. 2. Click Restore Factory Defaults & Format All Volumes. 3. Choose to restart or shut down the NAS after the system is reset. 4. Click OK.
Reinitialize the NAS	This deletes all data on the disks and reinstalls QTS.	1. Go to Control Panel > System > Backup/Restore > Restore to Factory Default. 2. Click Reinitialize NAS. 3. Choose to restart or shut down the NAS after the NAS is reinitialized. 4. Click OK.

External Device

USB Printer

The NAS supports using and sharing up to three network printers on your network in Windows, macOS, and Linux (Ubuntu) environments.

Configuring USB Printer Settings

Ensure that the printers are connected to the NAS via USB before performing this task.



Warning

Restarting the NAS or updating QTS while print jobs are still in progress cancels all the queued print jobs.

1. Go to **Control Panel > System > External Device > USB Printer**.
QTS displays the detected USB printers on your network.
2. Select a USB printer and then perform one or more of the following tasks.

Task	Action
View printer information	Click Printer Info . This displays the details of the selected printer.
View printer log	Click Printer Log . This displays the current and completed print jobs on the selected printer.  Tip You can stop, resume, or cancel ongoing or pending print jobs. You can also delete completed or pending print jobs. Click Clear to clear the history.

Clean up spool space	Click Clean Up Spool Space . This deletes the data stored in the printer spool.
Configure printer settings	Click Settings . This enables you to configure the following settings: • Stop printer sharing and clear print spool: Select this option to disable printing and delete all stored data on the selected printer. • Bonjour printer support: Select this option to introduce the printing service to the macOS users on your network.

- Optional: Specify the maximum number of print jobs allowed on each printer.
One printer can support processing up to 1000 print jobs. The oldest print jobs are automatically overwritten if the printer reaches the maximum number of print jobs.
- Click **Apply**.

Creating a USB Printer Access List

You can create an access list to allow or deny user access to USB printers.

- Go to **Control Panel > System > External Device > USB Printer**.
QTS displays the detected USB printers on your network.
- Specify access rights.
 - Beside **Access right**, select **Allow printing** or **Deny printing**.
 - Specify the IP addresses or domain names that you want to allow or deny.



Tip

You can specify multiple IP addresses or domain names and separate them using commas.
You can also use wildcard characters (such as an asterisk or a question mark) in an IP address or a domain name.

- Click **Apply**.

Uninterruptible Power Supply (UPS)

The NAS supports connecting to uninterruptible power supply (UPS) devices to protect the NAS from abnormal system shutdowns caused by power disruptions.

NAS Behavior During a Power Outage

The following table describes the possible scenarios during a power outage and the corresponding NAS behavior.

Phase	Scenario	NAS Behavior
Phase 1: From the start of the power outage until the end of the specified waiting time	The power outage occurs.	The NAS detects the remaining UPS power.
	The UPS power is greater than 15%.	Depending on your UPS settings, the NAS powers off or switches to auto-protection mode after the specified waiting time elapses.
	The UPS power is less than 15%.	After 30 seconds, the NAS automatically powers off or switches to auto-protection mode regardless of the specified waiting time.
	The power is restored.	The NAS remains functional.
Phase 2: From the end of the specified waiting time until the UPS runs out of power	The power is not restored, and the NAS is in auto-protection mode.	The NAS stops all running services. All shared folders and iSCSI LUNs become inaccessible.
	The power is not restored, and the NAS is powered off.	The NAS remains powered off.
	The power is restored, and the NAS is in auto-protection mode.	The NAS restarts and resumes its previous state.
	The power is restored, and the NAS is powered off.	The NAS remains powered off.
Phase 3: From the moment the UPS runs out power until the power is restored	The power is not restored, and the NAS is in auto-protection mode.	The NAS powers off.
	The power is not restored, and the NAS is powered off.	The NAS remains powered off.
	The power is restored.	The NAS applies the specified power recovery settings.

Configuring the UPS Settings

1. Go to **Control Panel > System > External Device > UPS**.
2. Select one of the following options and configure the settings.

Mode	Steps
USB connection	a. Connect the UPS to the NAS using a USB cable. b. Select USB connection. c. Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the NAS to enter auto-protection mode after the power fails for a specified time period  Note In auto-protection mode, the NAS stops all services and unmounts all volumes to

	protect your data. After the power is restored, the NAS restarts and resumes normal operation. d. (Optional) Select Enable network UPS master and then specify the IP addresses to which QTS sends notifications in the event of power failure.  Note This option can only be selected when the UPS is connected to the NAS via USB.
SNMP connection	a. Connect the UPS to the same network as the NAS. b. Select SNMP connection. c. Specify the IP address of the UPS. d. Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the NAS to enter auto-protection mode after the power fails for a specified time period
Network UPS slave	a. Connect the UPS to the same network as the NAS. b. Select Network UPS slave. c. Specify the IP address of the UPS server. d. Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the NAS to enter auto-protection mode after the power fails for a specified time period

3. Click **Apply**.

System Status

You can check the status of your NAS in **Control Panel > System > System Status**.

Section	Description
System Information	This screen displays basic system information, such as model name, CPU, memory, firmware version, and system up time.
Network Status	This screen displays the current network settings of each network interface.

Section	Description
System Service	This screen displays the current status of system services, such as antivirus, domain controllers, multimedia management, and VPN servers.
Hardware Information	This screen displays NAS hardware information, such as CPU usage, memory, disk temperature, and system fan speed.

System Logs

You can view and manage system logs in **Control Panel > System > System Logs**.

System Event Logs

QTS keeps a maximum of 10,000 event log entries, including warnings, errors, and information messages. You can perform the following actions for System Event Logs.

Action	Steps
Display a certain event type	Select an event type from the drop-down list.
Perform a basic search	Specify keywords in the search box.
Perform an advanced search	1. Click  beside the search box. 2. Specify the detailed information. 3. Click Search.
Delete a log entry	Right-click a log entry and then select Delete this record .
Copy one or more log entries	1. Select one or multiple log entries. 2. Right-click the selected log entries. 3. Click Copy.  Tip You can press Ctrl or Shift to select multiple log entries.
Delete all event log entries	1. Click Clear All. A confirmation message appears. 2. Click OK.
Export system event logs	Click Save . QTS exports system event logs as a CSV file and downloads the file to your computer.

System Connection Logs

QTS can log the following events for connection sessions.

Protocol	Events
HTTP/HTTPS, FTP, Telnet, SMB, iSCSI, RADIUS	• Logging on and off • Accessing, creating, deleting, moving, and renaming files and folders

Protocol	Events
AFP and SSH	Logging on and off

You can perform the following actions for System Connection Logs.

Action	Steps
Start logging connection sessions	Click Start Logging .
Configure log settings	1. Click Options. 2. Select which connection types to log. 3. (Optional) Choose to archive the connection logs to a specified location when the number of log entries reaches 10,000. 4. Click Apply.
Display a certain event type	Select an event type from the drop-down list.
Perform a basic search	Specify keywords in the search box.
Perform an advanced search	1. Click  beside the search box. 2. Specify the detailed information. 3. Click Search.
Delete a log entry	Right-click a connection log entry and then select Delete this record .
Block a connection	1. Right-click a connection log entry. 2. Hover the mouse pointer over Add to the block list. 3. Select a time period for which the connection will be blocked.
Delete all connection log entries	1. Click Clear All. A confirmation message appears. 2. Click OK.
Export system event logs	Click Save . QTS exports and downloads the system connection logs as a CSV file.

Online Users

This section shows the users that are currently connected to the NAS via various network services. You can perform the following actions.

Action	Step
Disconnect a connection	Right-click a user connection and select Disconnect this connection .
Block a connection	1. Right-click a user connection and select Add to the block list. 2. Specify how long the connection should be blocked.

Action	Step
Disconnect and block a connection	1. Right-click a user connection and select Disconnect this connection and block the IP. 2. Specify how long the connection should be blocked.
Perform a basic search	Specify keywords in the search box.
Perform an advanced search	1. Click  beside the search box. 2. Specify the detailed information. 3. Click Search.

Syslog Client Management

Syslog is a standard for forwarding log messages on a network. You must enable this service to store event and connection logs on a remote syslog server. You can select the types of logs to record.

Resource Monitor

You can monitor the status of your NAS in **Control Panel > System > Resource Monitor**.

Resource Monitor displays information and statistics about hardware usage and system resources.

Section	Description
Overview	This screen provides a general summary of CPU usage, memory usage, network usage, and ongoing processes on the NAS.
System Resource	This screen uses line charts to display CPU usage, memory usage, network usage, and graphics card usage (if supported and installed) over time. You can hover the mouse pointer over a line chart to view the hardware usage at a specific point in time.  Tip You can click More () and then select Settings to specify the time interval on the line charts.
Storage Resource	This screen uses line charts to display the activities of volumes, LUNs, storage pools, RAID groups, and disks on the NAS over time. This screen also summarizes the storage usage of each volume. You can hover the mouse pointer over a line chart to view the storage activity at a specific point in time.

Section	Description
Processes	This screen displays all ongoing background processes and provides information about each process, such as its current status, CPU usage, and memory usage.  Tip You can enable Group by Applications to group related processes together (for example, all the processes related to an application or a system feature).

5. Privilege

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

Users

Default User Accounts

User Account	Description
admin	This account can configure settings, create users, and install applications. You cannot delete this account.

Creating a Local User

1. Go to **Control Panel > Privilege > Users**.
2. Click **Create > Create a User**.
The **Create a User** window appears.
3. Specify the following information.

Field	Description
Profile photo	Optional: Upload a profile photo for the user.
User Description (optional)	Specify a user description that contains a maximum of 50 characters.
Username	Specify a username that contains 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: . - _ ~ ! @ # \$ % ^ & () { }
Password	Specify a password that contains a maximum of 64 ASCII characters.
Phone number (optional)	Specify a phone number that will receive SMS notifications from QTS. For details, see SMS Notifications .  Note Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.

Field	Description
Email (optional)	Specify an email address that will receive notifications from QTS. For details, see Email Notifications.  Note Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
Send a notification mail to the newly created user (optional)	When selected, QTS sends a message that contains the following information to the specified email address: • Username and password • URLs for connecting to the NAS  Tip Users have the option to edit the notification message. To edit the notification message, follow these steps: - Click Edit Message. The Edit Message window appears. - Specify a subject and message. - Click Save. - Optional: To use the default message, click Restore to Defaults.

- Specify the user's user groups, shared folder permissions, or application privileges.
For details, see [Modifying User Account Information](#).

- Click **Create**.

Creating Multiple Users

- Go to **Control Panel > Privilege > Users**.
- Click **Create > Create Multiple Users**.
The **Multiple Users Creation Wizard** appears.
- Click **Next**.
- Specify the following information.

Field	Description
User Name Prefix	Specify a username that contains a maximum of 23 ASCII characters and that does not: • Contain a space • Begin with the following characters: - # @ • Contain the following characters: @ " + = / \ : * ? < > ; [] % ` , This prefix will be included before all usernames. Example: test
User Name Start No	Specify a start number with a maximum of 8 digits. Example: 1  Note QTS removes leading zeros in starting numbers. For example, 001 becomes 1.
Number of Users	Specify the number of users (1 to 4095). Example: 5
Password	Specify a password that contains a maximum of 64 ASCII characters.

**Note**

The username format is [username prefix][user number]. The specified start number and number of users determine the user number.
Using the examples, the users created will have the following usernames: test1, test2, test3, test4, and test5.

5. Click **Next**.
The **Create Private Network Share** screen appears.
6. Optional: Create a private network share for each user.
 - a. Select **Yes**.
 - b. Click **Next**.
 - c. Specify the following information.

Field	Description
Hide network drive	Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
Disk Volume	Select the data volume where the private network share will be created.

To continue without creating a private network share, select **No**.

7. Click **Next**.
QTS creates the user accounts and adds them to the displayed user list.

- Click **Finish**.

User Account Lists

The NAS supports importing user accounts from TXT, CSV, and BIN files. The files contain user account information including usernames, passwords, user groups, and quota settings.

File Format	Description
TXT	Create user account lists using a text editor. For details, see Creating a TXT User File .
CSV	Create user account lists using a spreadsheet editor. For details, see Creating a CSV User File .
BIN	QNAP NAS devices can export user account information, including quota settings, to BIN files. For details, see Exporting Users .

Creating a TXT User File

- Create a new file in a text editor.
- Specify user information in the following format.
Username,Password,Quota (MB),Group Name



Important

- Separate values using commas.
- Specify a quota between 100 MB and 2048 GB (2048000 MB).



Note

The system only accepts quotas in MB. GB values must be expressed in MB.

- Specify information for only one user on each line.

Example:

```
John,s8fk4b,100,Sales
Jane,9fjwbx,150,Marketing
Mary,f9xn3ns,390,RD
```

- Save the list as a TXT file.



Important

If the list contains multi-byte characters, save the file with UTF-8 encoding.

Creating a CSV User File

- Create a new workbook in a spreadsheet editor.
- Specify user information in the following format.
 - column A: Username
 - column B: Password
 - column C: Quota (MB)
 - column D: Group name

**Important**

- Specify a quota between 100 MB and 2048 GB (2048000 MB).

**Note**

The system only accepts quotas in MB. GB values must be expressed in MB.

- Specify information for only one user in each row.
Example:

	A	B	C	D
1	John	s8fk4b	100	Sales
2	Jane	9fjwbx	150	Marketing
3	Mary	f9xn3ns	390	R&D

- Save the workbook as a CSV file.

**Important**

If the list contains multi-byte characters, open the file using a text editor and then save with UTF-8 encoding.

Importing Users

- Go to **Control Panel > Privilege > Users**.
- Click **Create > Import/Export Users**.
The **Import/Export Users** window appears.
- Select **Import user and user group settings**.
- Optional: Select any of the following options.

Field	Description
Send a notification mail to the newly created user	When selected, QTS sends a message that contains the following information to the specified email address of the user. - Username and password - URLs for connecting to the NAS  Important To send email notifications, ensure that you have configured an SMTP server. For details, see Configuring an Email Notification Server.
Overwrite duplicate users	When selected, QTS overwrites existing user accounts that have duplicates on the imported user account list.

- Click **Browse**, and then select the file that contains the user account list.

**Important**

Ensure that you are importing a valid QTS user account list file to avoid parsing errors.

For details, see [User Account Lists](#).

6. Click **Next**.

File Type	User Action
TXT or CSV	The Import User Preview screen appears. Check the status of the user account list.  Important The Status indicates whether any information is invalid. If any information is invalid, the user account list will not be imported successfully.
BIN	The following screen describes the Overwrite duplicate users feature.

7. Click **Next**.

QTS imports the user account list.

8. Click **Finish**.

Exporting Users

1. Go to **Control Panel > Privilege > Users** .

2. Click **Create > Import/Export Users** .
The **Import/Export Users** window appears.

3. Select **Export user and user group settings**.

4. Click **Next**.
QTS exports the user account list to your computer as a BIN file.



Tip

You can use this file to import users to another NAS running QTS.

Modifying User Account Information

1. Go to **Control Panel > Privilege > Users** .

2. Locate a user.

3. Perform any of the following tasks.

Task	User Action
Change password	a. Under Action, click  . The Change Password window appears. b. Specify a password that meets the requirements. c. Verify the password.

Task	User Action
Edit account profile	a. Under Action, click . The Edit Account Profile window appears. b. Edit the settings. The Edit Account Profile window provides the following settings not included in the Create a User window: • Description (optional): Specify a user description that contains a maximum of 50 characters. • Disallow the user to change password: When selected, QTS prevents the user from changing the password. • Disable this account: Select this option to disable the user account. You can either select to disable the account Now or specify an Expiry Date.
Edit user group membership	a. Under Action, click . The Edit User's Groups window appears. b. Select or deselect user groups. For details, see User Groups.
Edit shared folder permissions	a. Under Action, click . The Edit Shared Folder Permission window appears. b. Edit the user's permissions for each shared folder. For details, see Shared Folder Permissions.
Edit application privileges	a. Under Action, click . The Edit Application Privileges window appears. b. Select the applications that the user is allowed to access.  Tip QNAP recommends denying access to applications and network services that the user does not require. By default, administrator accounts have access to all applications.

4. Click **Apply**.

Deleting Users

1. Go to **Control Panel > Privilege > Users**.
2. Select the users to delete.



Note

Default user accounts cannot be deleted.

3. Click **Delete**.
A warning message appears.
4. Optional: Select **Also delete the selected user(s)' home folders and data**.

5. Click **Yes**.

Home Folders

Enabling home folders creates a personal folder for each local and domain user on the NAS. Users can access their home folder through Microsoft networking, FTP, and File Station.

All home folders are located in the homes shared folder. By default, only the administrator can access this folder.

Enabling Home Folders

1. Go to **Control Panel > Privilege > Users**.
2. Click **Home Folder**.
The **Home Folder** window appears.
3. Select **Enable home folder for all users**.
4. Select a volume.
The volume is used to store the home folders.
5. Click **Apply**.

User Groups

A user group is a collection of users with the same access rights to files or folders. Administrators can create user groups to manage folder permissions for multiple users.

Default User Groups

User Group	Description
administrators	Users in this group can configure settings, create users, and install applications. You cannot delete this group.
everyone	Users in this group can only view and modify files. This group contains all local user accounts and can be used to grant shared folder permissions to all local user accounts. You cannot delete this group.

Creating a User Group

1. Go to **Control Panel > Privilege > User Groups**.
2. Click **Create**.
The **Create a User Group** window appears.
3. Specify the following information.

Field	Description
User group name	Specify a user group name that contains 1 to 128 ASCII characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Dashes (-)
Description	Specify a description that contains a maximum of 128 ASCII characters.

4. Optional: Add users to the user group.
 - a. Under **Assign users to this group**, click **Edit**.
 - b. Select one or more users.
5. Specify shared folder permissions for the user group.
 - a. Under **Edit shared folder permissions**, click **Edit**.
 - b. Select the permissions for each shared folder.
For details, see [Conflicts in Shared Folder Permissions](#).
6. Click **Create**.

Modifying User Group Information

1. Go to **Control Panel > Privilege > User Groups**.
2. Locate a user group.
3. Perform any of the following tasks.

Task	User Action
Edit the user group description	a. Under Action, click . The View Group Details window appears. b. Modify the description.
Edit a user group	a. Under Action, click . The Edit User Group window appears. b. Select or deselect user groups.

Task	User Action
Edit shared folder permissions	a. Under Action, click . The Edit Shared Folder Permissions window appears. b. Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions.  Important Group-level permissions may override user-level permissions. For details, go to Conflicts in Shared Folder Permissions.

4. Click **OK**.

Deleting User Groups

1. Go to **Control Panel > Privilege > User Groups**.
2. Select the user groups to delete.



Note

Default user groups cannot be deleted.

3. Click **Delete**.
A warning message appears.
4. Click **OK**.

Shared Folders

Go to **Control Panel > Privilege > Shared Folders** to configure settings and permissions for shared folders.

Default Shared Folders

QTS automatically creates the following shared folders to help you organize data on your NAS.



Important

Default shared folders cannot be deleted and certain properties cannot be changed.

Folder	Description
Download	This is the default folder for Download Station and is the default path when downloading content in QTS. You can assign a different path for downloads in Download Station.
Multimedia	This is the default folder for multimedia apps and stores multimedia content such as photos, videos, and music. You can manage this folder in the Multimedia Management utility in Control Panel.
Public	This folder can be used by any user account. By default, the shared folder permission for this folder is set to Read Only. For details, see Shared Folder Permissions .
Web	This folder stores content from the Web Server utility, which you can manage in Control Panel.

Restoring Default Shared Folders

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Click **Restore Default Shared Folders**.
A warning message appears.
3. Click **OK**.

QTS restores the default shared folders.

Creating a Shared Folder

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Click **Create**, and then select **Shared Folder**.
The **Create A Shared Folder** window opens.
3. Specify the following information.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' "
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Disk Volume	Specify the volume on the NAS where the shared folder will be created.
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier. This setting is only available if you select a Qtier-enabled storage pool.  Note Users can also enable auto-tiering from the Shared Folders screen.
Path	You can specify a path or allow QTS to automatically create one.

4. Optional: Configure user access permissions.
 - a. Under **Configure access privileges for users**, click **Edit**.
 - b. Specify the access permissions for users.
For details, see [Shared Folder Permissions](#).
5. Optional: Enable folder encryption.
 - a. Under **Folder Encryption**, click **Edit**.
 - b. Select **Encryption**.

Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.

- c. Specify the following information.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " \$: = \ This field does not support multibyte characters.
Verify Password	The password must match the previously specified password.
Save encryption key	When enabled, QTS automatically unlocks the shared folder after the NAS restarts. When disabled, the administrator must unlock the folder after the NAS restarts. For details, see Unlocking a Shared Folder .

6. Optional: Configure advanced settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Media Folder	Selecting this option allows media applications to scan this folder for media files.
Hide network drive	Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	This option is available only when Network Recycle Bin is enabled. Selecting this option prevents non-administrator users from recovering and deleting files in the Recycle Bin.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is not visible if Qsync is not installed on the NAS.
Enable access-based share enumeration (ABSE)	When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders.
Enable access-based enumeration (ABE)	When enabled, users can only see the files and folders that they have permission to access.

Option	Description
Set this folder as the Time Machine backup folder (macOS)	When enabled, the shared folder becomes the destination folder for Time Machine in macOS.

- Click **Create**.

Editing Shared Folder Properties

- Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
- Locate a shared folder.
- Under **Action**, click .
The **Edit Properties** window appears.
- Modify any of the following settings.

Option	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: - Begin or end with a space - Contain consecutive spaces - End with "." - Begin with "_sn_" or "_sn_bk" - Contain the following characters: " + = / \ : * ? < > ; [] % ` ' "
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters. The information is for your reference and is not used by QTS.
Disk Volume	Specify the volume on the NAS where the shared folder will be created.
Path	You can specify a path or allow QTS to automatically create one.
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier . This setting is only available if the folder is in a Qtier-enabled storage pool.  Note Users can also enable auto-tiering from the Shared Folders screen.
Media Folder	Selecting this option allows media applications to scan this folder for media files.
Hide network drive	Selecting this option hides the folder in Windows networks. Users that know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.

Option	Description
SMB Encryption	This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycling Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now.	This option is available only when Network Recycle Bin is enabled. Selecting this option prevents non-administrator users from recovering and deleting files in the Recycle Bin.
Enable write-only access on FTP connection	Selecting this option gives the administrator exclusive read and write access to the shared folder. Non-administrator users connected through FTP only get write access.
Only allows applications to access files using the long file name format	When selected, applications can only use the long file name (LFN) format to access files in the shared folder.
Encrypt this folder	Selecting this option enables folder encryption, which protects folder content against unauthorized data access when the drives are physically stolen.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is not visible if Qsync is not installed on the NAS.
Enable access-based share enumeration (ABSE)	When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders.
Enable access-based enumeration (ABE)	When enabled, users can only see the files and folders that they have permission to access.
Set this folder as the Time Machine backup folder (macOS)	When enabled, the shared folder becomes the destination folder for Time Machine in macOS.
Migrate to Snapshot Shared Folder	Clicking this button opens the Migrating shared folder to a snapshot shared folder wizard, which allows you to migrate the shared folder to a snapshot shared folder. For details, see Migrating to a Snapshot Shared Folder .

5. Click **OK**.

Refreshing a Shared Folder

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Locate a shared folder.
3. Under **Action**, click .

Removing Shared Folders

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Select the shared folders to remove.



Note

Default shared folders cannot be removed.

3. Click **Remove**.
A warning message appears.
4. Optional: Select **Also delete the data (mounted ISO image files will not be deleted)**.
5. Click **Yes**.

Snapshot Shared Folders

A snapshot shared folder is a shared folder created on a dedicated volume, which allows users to quickly recover data by restoring a folder or reverting a volume from a snapshot. Users can also set folder quotas for snapshot shared folders. For details on snapshots, see [Storage & Snapshots](#).

The snapshot shared folder feature requires a NAS that supports snapshots and contains at least 1 GB of memory. For details on compatible models, see www.qnap.com/solution/snapshots.

Creating a Snapshot Shared Folder

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Click **Create**, and then select **Snapshot shared folder**.
The **Create a Snapshot Shared Folder** window opens.
3. Specify the following information.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' "
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Storage Pool	Specify the storage pool on the NAS where the snapshot shared folder will be created.
Space Allocation	Select whether the storage pool will have thick or thin provisioning. For details, see Volumes .
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier . This setting is only available if you select a Qtier-enabled storage pool.  Note Users can also enable auto-tiering from the Shared Folders screen.
Allocate folder quota	You can allocate a folder quota for the snapshot shared folder.

4. Optional: Configure user access permissions.
 - a. Under **Configure access privileges for users**, click **Edit**.

- b. Specify the access permissions for users.
For details, see [Shared Folder Permissions](#).
5. Optional: Configure advanced settings.
For details, see [Creating a Shared Folder](#).
6. Click **Create**.

Migrating to a Snapshot Shared Folder

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Select the folder you want to migrate to a snapshot shared folder.
3. Click **Migrate to Snapshot Shared Folder**.
The **Migrating shared folder to a snapshot shared folder** wizard appears.
4. Select the location for the snapshot shared folder.
5. Click **Next**.
6. Optional: Free up storage pool space on the volume.



Note

If there is not enough storage space in the storage pool for the snapshot shared folder, the **Free Storage Pool Space** screen appears.

Option	User Action
Release unused guaranteed snapshot space	 Note This option is only available if guaranteed snapshot space has been allocated to the storage pool. a. Click Set up now. The Snapshot Settings window appears. b. Configure the snapshot settings to release space. For details, see Storage & Snapshots. c. Click OK.
Run a space reclaim to release used space on thin volumes	 Note This option is only available if the storage pool contains a thin volume with reclaimable space. a. Click Run now. A dialog box appears. b. Click OK to reclaim the available storage space. QTS reclaims the used space. A dialog box appears. c. Click OK.

Option	User Action
Convert a thick volume to a thin volume to release unallocated space	 Note This option is only available if the storage pool contains a thick volume. - Select a volume to convert. - Click Run now. The Convert to Thin Volume window appears.  Warning Converting a volume deletes all existing snapshots on the volume. - Click Apply. QTS converts the volume.

7. Configure the snapshot shared folder.

Option	Description
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier. This setting is only available if you select a Qtier-enabled storage pool.  Note Users can also enable auto-tiering from the Shared Folders screen.
Space Allocation	Select whether the volume will have thick or thin provisioning. For details, see Volumes .
Allocated space quota	Specify a quota for the snapshot shared folder.  Tip Click Set to Max to allocate all remaining storage pool space to the volume.

8. Click **Next**.

9. Review the settings.

10. Click **OK**.

ISO Shared Folders

Users can mount ISO image files on the NAS as ISO shared folders and access them without having to burn discs. The NAS supports up to 256 mounted ISO shared folders.

ISO Shared Folder Requirements

By default, most NAS models can support up to 256 ISO shared folders. However, some NAS models support fewer than 256 ISO image files, depending on the number of Network Recycle Bin folders: Number of supported ISO image files = 256 – 6 (default shared folders) – (number of Network Recycle Bin folders). The following NAS models support fewer than 256 ISO image files.

NAS Model		
TS-1x: • TS-110 • TS-112 • TS-119 • TS-119P+ • TS-120 • TS-121	TS-2x: • TS-210 • TS-212 • TS-219 • TS-219P • TS-219P+ • TS-220 • TS-221	Other models: • TS-410

Mounting an ISO File as a Shared Folder

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Click **Create**, and then select **Create an ISO Share**.
The **Create an ISO Share** window opens.
3. Select the source ISO image file to be mounted.
4. Click **Next**.
5. Specify the following information.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • End with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' "  Note For ARM-based NAS models, ISO shared subfolder names do not support Cyrillic characters. If a subfolder name includes Cyrillic characters, it will not be displayed correctly on the NAS. Shared folders on macOS that include the character "#" in their names cannot be mounted.
Hidden Folder	Selecting Yes hides the folder in Windows networks. Users who know the specific path can still access the folder.
Description	Specify a description that contains a maximum of 128 ASCII characters.

6. Click **Next**.

7. Configure user access permissions and guest access rights to the ISO shared folder.

Type	Option	Description	User Action
User access permissions	Grant read-only access right for administrators only	Selecting this option grants administrator accounts read-only access to the ISO shared folder.	a. Click Next . b. Review the settings.
	By User	Selecting this option allows you to configure access permissions to the ISO shared folder at the user level.	a. Click Next . b. Configure the user account access rights for the ISO shared folder. c. Click Next . d. Review the settings.
	By User Group	Selecting this option allows you to configure access permissions to the ISO shared folder at the user group level.	a. Click Next . b. Configure the user group access rights for the ISO shared folder. c. Click Next . d. Review the settings.
Guest access rights	Deny Access	Selecting this option denies access to guest accounts.	N/A
	Read only	Selecting this option grants read-only access to guest accounts.	

For details, see [Shared Folder Permissions](#).

8. Click **Next**.

QTS mounts the ISO file as a shared folder and then adds it to the **Shared Folder** screen.

9. Click **Finish**.

Shared Folder Permissions

Permission	Description
Read Only (RO)	The user or user group can read files in the shared folder, but not write them.
Read/Write (RW)	The user or user group can read and write files in the shared folder.
Deny	The user or user group cannot read or write files in the shared folder.



Note

You can configure shared folder permissions for users and user groups. For details, see the following topics:

- [Modifying User Account Information](#)

• Modifying User Group Information

Editing Shared Folder Permissions

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Locate a shared folder.
3. Under **Action**, click .
The **Edit Shared Folder Permission** window appears.
4. Under **Select permission type**, select a permission type to edit.
5. Perform any of the following tasks.

Permission Type	Description	User Action
Users and groups permission	Edit user and user group permissions for shared folders that can be accessed through Windows, macOS, FTP, and File Station.	a. Specify permissions for each user and user group. b. Optional: Add a user to the list of users with permissions for the shared folder. 1. Click Add. The Select users and groups window appears. 2. Select the type of user or user group from the drop-down menu in the upper left. 3. Select the permissions for the users you want to add. 4. Click Add. QTS adds the users and their corresponding permissions to the list. c. Optional: Remove a user from the list of users with permissions for the shared folder. 1. Click the user you want to remove. 2. Click Remove. QTS removes the user from the list. d. Optional: Modify guest access rights. Under Guest Access Right, select the permission type for guest accounts.

Permission Type	Description	User Action
NFS host access	Edit NFS host access rights for shared folders.	- Select the Access right to enable NFS access rights. - Under Host / IP / Network, enter an IP address or domain name. - Optional: Add an NFS host. Under Allowed IP Address or Domain Name, click Add. QTS adds an entry to the list. - Optional: Delete an NFS host. - Select an NFS host from the list. - Click Delete. QTS removes the host from the list.
Microsoft Networking host access	Specify which computers can access shared folders through Microsoft Networking.	- Add a Microsoft Networking host. Click Add. QTS adds an entry to the list. - Under Host / IP / Network, enter an IP address or domain name. - Optional: Delete a Microsoft Networking host. - Select a Microsoft Networking host from the list. - Click Delete. QTS removes the host from the list.

6. Click **Apply**.

Configuring Advanced Folder Permissions

- Go to **Control Panel > Privilege > Shared Folders > Advanced Permissions**.
- Select any of the following options.

Option	Description
Enable Advanced Folder Permissions	When enabled, users can assign folder and subfolder permissions to individual users and user groups.
Enable Windows ACL support	When enabled, users can only configure folder and subfolder permissions from Windows File Explorer.

3. Click **Apply**.

Conflicts in Shared Folder Permissions

When a user is assigned different permissions for a shared folder, QTS uses the following hierarchy to resolve conflicts.

- No Access/Deny
- Read/Write (RW)

3. Read Only (RO)

User Permission	User Group Permission	Actual Permission
No Access	No Access	No Access
Read Only		No Access
Read/Write		No Access
Not Specified		No Access
No Access	Read Only	No Access
Read Only		Read Only
Read/Write		Read/Write
Not Specified		Read Only
No Access	Read/Write	No Access
Read Only		Read/Write
Read/Write		Read/Write
		• Shared folders through Samba/AFP: Read/Write • Shared folders through NFS: Read Only
Not Specified		Read/Write
No Access	Not Specified	No Access
Read Only		Read Only
Read/Write		Read/Write
Not Specified		No Access

Shared Folder Access

You can map or mount a NAS shared folder as a network drive, allowing you to easily access and manage files from your Windows, Mac, or Linux computer.

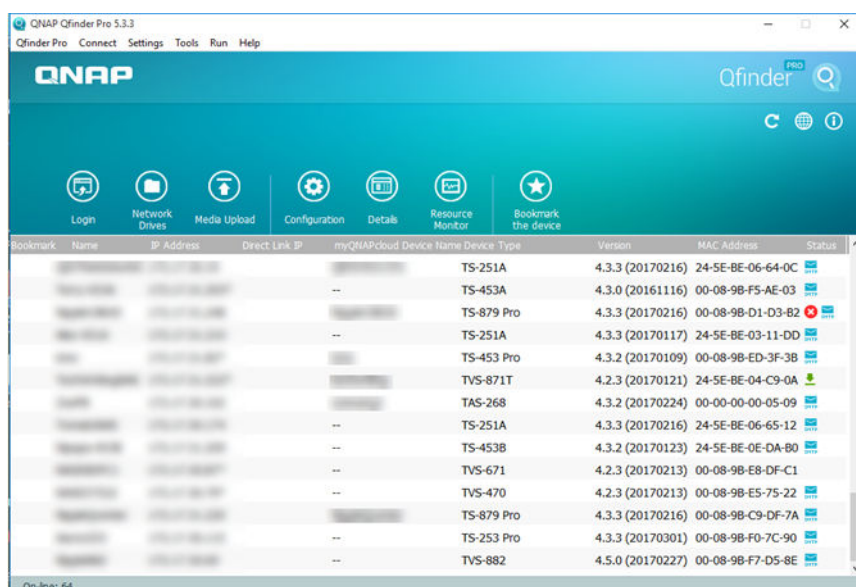
For Windows and Mac, you can use Qfinder Pro to map or mount your NAS shared folders. Qfinder Pro is a desktop utility that enables you to locate and access the QNAP NAS devices in your local area network.

To download Qfinder Pro, go to <https://www.qnap.com/utilities>.

Mapping a Shared Folder on a Windows Computer

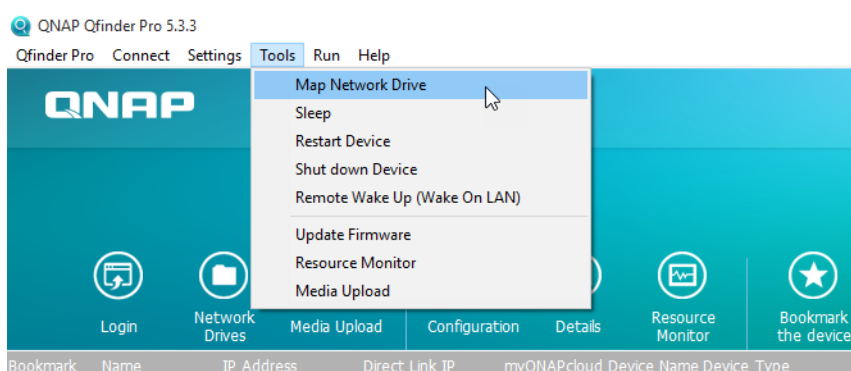
Before mapping a shared folder, ensure that you have Qfinder Pro installed on your Windows computer.

1. Power on the NAS.
2. Connect the NAS to your local area network.
3. Open **Qfinder Pro**.
Qfinder Pro displays all QNAP NAS devices in your local area network.



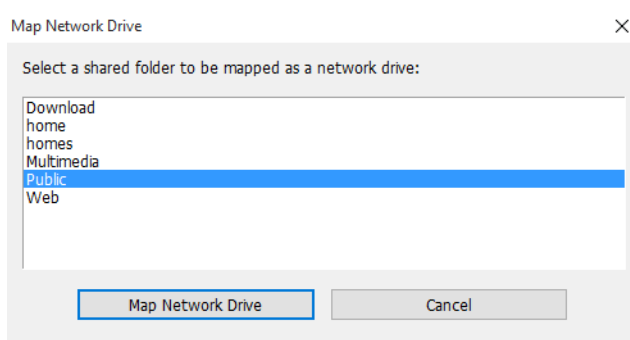
4. Select the NAS where the shared folder is located.

5. Click **Tools > Map Network Drive**.

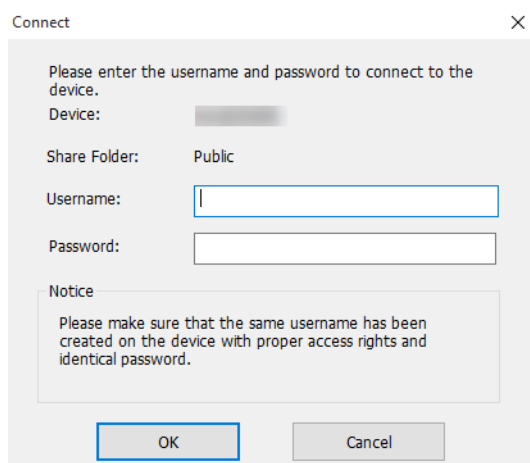


6. Select a shared folder.

7. Click **Map Network Drive**.



8. Specify your QTS username and password.

9. Click **OK**.


Connect

Please enter the username and password to connect to the device.

Device: [Redacted]

Share Folder: Public

Username: [Text Box]

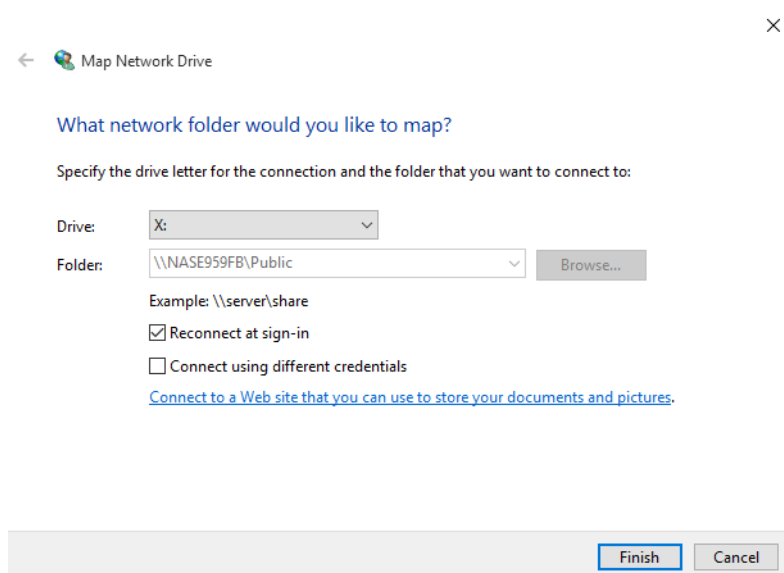
Password: [Text Box]

Notice

Please make sure that the same username has been created on the device with proper access rights and identical password.

OK Cancel

10. Specify the following information.



← Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: X: [Dropdown]

Folder: \\NASE959FB\Public [Dropdown] Browse...

Example: \\server\share

☒ Reconnect at sign-in

☐ Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

Finish Cancel

Field	Description
Drive	Specify the drive letter for the shared folder.
Folder	This field is uneditable because you have already selected the shared folder. This is for your reference.
Reconnect at sign-in	When selected, the shared folder will automatically be connected the next time the user signs in.
Connect using different credentials	When selected, the user will have the option to sign into the NAS with a different account after mapping the shared folder.
Connect to a Web site that you can use to store your documents and pictures.	When clicked, the Add Network Location Wizard appears. You can use this wizard to create a shortcut to your mapped shared folder.

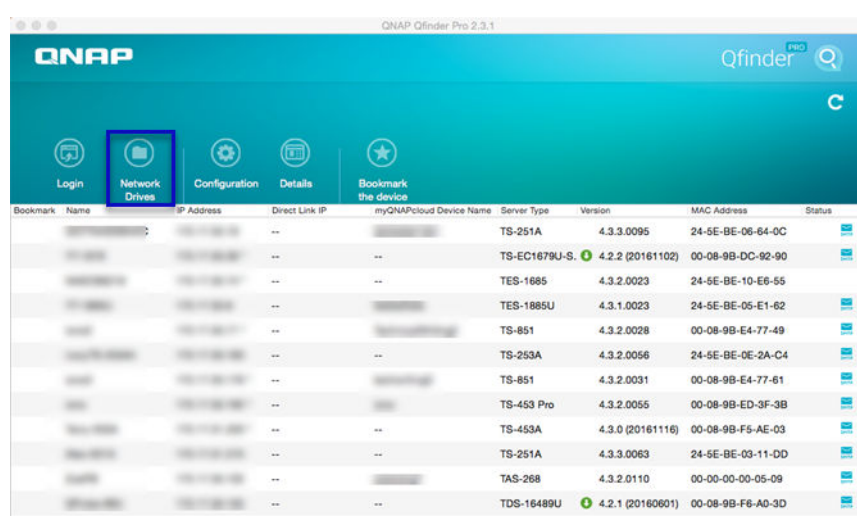
11. Click **Finish**.

The shared folder is mapped as a network drive and can be accessed using Windows Explorer.

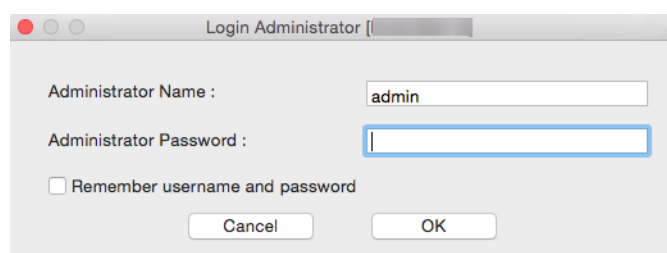
Mounting a Shared Folder on a Mac Computer

Before mounting a shared folder, ensure that you have Qfinder Pro installed on your Mac computer.

1. Power on the NAS.
2. Connect the NAS to your local area network.
3. Open **Qfinder Pro**.
Qfinder Pro displays all QNAP NAS devices in your local area network.
4. Select the NAS where the shared folder is located.
5. Click **Network Drives**.

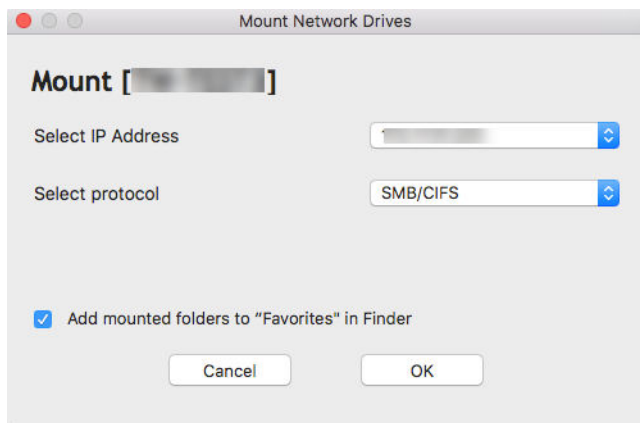


6. Specify your QTS username and password.
7. Click **OK**.



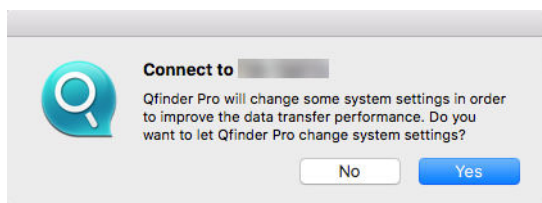
The **Mount Network Drives** window opens.

8. Select **Add mounted folders to "Favorites" in Finder**.
9. Click **OK**.

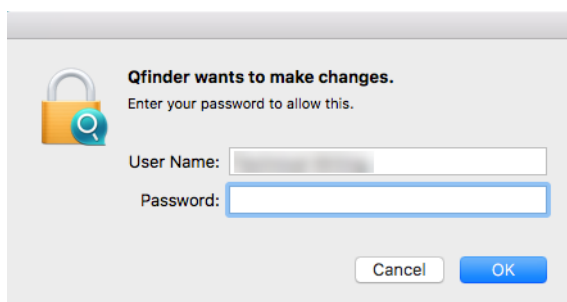


A confirmation message appears.

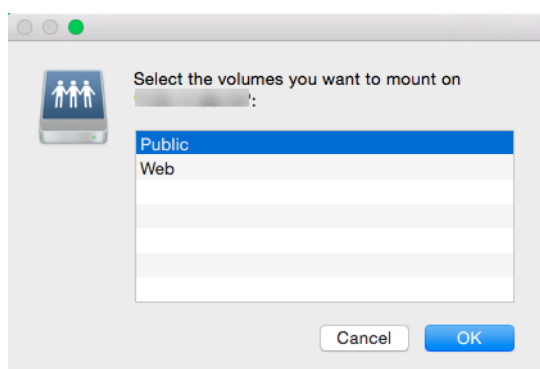
10. Click **Yes**.



11. Specify your Mac username and password.
12. Click **OK**.



13. Select the shared folder.
14. Click **OK**.



The shared folder is mounted as a network drive and can be accessed using Qfinder Pro.

Mounting a Shared Folder on a Linux Computer

1. Open a terminal with root privileges.
2. Run the following command:

```
mount <NAS Ethernet Interface IP>:/share/<Shared Folder Name> <Directory to Mount>
```



Tip

If the NAS ethernet interface IP address is 192.168.0.42 and you want to connect to a shared folder "public" under the /mnt/pub directory, run the following command:

```
mount -t nfs 192.168.0.42:/share/public/mnt/pub
```

3. Specify your NAS username and password.

You can connect to the shared folder using the mounted directory.

Folder Aggregation

Users can aggregate shared folders on a Windows network and link them to a portal folder accessible on the NAS. You can link up to 10 folders to a single portal folder.

Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation** to enable folder aggregation.



Note

- Folder aggregation is supported in Samba networks only. QNAP recommends folder aggregation for a Windows Active Directory (AD) environment.
- If access permissions are assigned to portal folders, the NAS and remote servers must be joined to the same AD domain.

Creating a Portal Folder



Note

Ensure that folder aggregation is enabled before performing the following steps. For details, see [Folder Aggregation](#).

1. Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation**.

2. Under **Folder Aggregation List**, click **Create a Portal Folder**.
The **Create a Portal Folder** window appears.
3. Specify the following information.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' "
Hidden Folder	Selecting Yes hides the folder in Windows networks. Users who know the specific path can still access the folder.
Comment	Specify a comment between 1 and 128 ASCII characters.
Users must login before accessing the portal folder.	When selected, users must log in to the NAS with their username and password before accessing the portal folder. This prevents guest accounts from accessing the portal folder and other user permission issues.

4. Click **Apply**.

Modifying Portal Folder Information



Note

Ensure that folder aggregation is enabled before performing the following steps. For details, see [Folder Aggregation](#).

1. Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation**.
2. Locate a portal folder.
3. Perform any of the following tasks.

Task	User Action
Edit portal folder properties	a. Under Action, click . The Edit Portal Folder window appears. b. Edit the folder properties. For details, see Creating a Portal Folder.
Configure the remote folder link	a. Under Action, click . The Remote Folder Link window appears. b. Specify the Name, Host Name, and Remote Shared Folder for any remote folder link.

4. Click **Apply**.

Deleting Portal Folders



Note

Ensure that folder aggregation is enabled before performing the following steps. For details, see [Folder Aggregation](#).

1. Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation**.
2. Select the portal folders that you want to delete.
3. Click **Delete**.
A warning message appears.
4. Click **Yes**.

Importing Folder Trees



Note

Ensure that folder aggregation is enabled before performing the following steps. For details, see [Folder Aggregation](#).

1. Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation**.
2. Click **Import/Export Folder Tree**.
The **Import/Export Folder Tree** window appears.
3. Under **Import Folder Tree**, click **Browse**.
4. Select the file that contains the folder tree.



Important

Ensure that you are importing a valid QTS folder tree file to avoid parsing errors.

5. Click **Import**.
A warning message appears.
6. Click **OK**.
QTS imports the folder tree.
7. Click **OK**.
8. Click **Finish**.

Exporting Folder Trees



Note

Ensure that folder aggregation is enabled before performing the following steps. For details, see [Folder Aggregation](#).

1. Go to **Control Panel > Privilege > Shared Folders > Folder Aggregation**.
2. Click **Import/Export Folder Tree**.
The **Import/Export Folder Tree** window appears.
3. Under **Export Folder Tree**, click **Export**.
QTS exports the folder tree to your computer as a BIN file.

**Tip**

You can use this file to import folder trees to another NAS running QTS.

4. Click **Finish**.

Shared Folder Encryption

Shared folders on the NAS can be encrypted with 256-bit AES encryption to protect data. Encrypted shared folders can be mounted with normal read/write permissions but can only be accessed using the authorized password. Encrypting shared folders protects sensitive data from unauthorized access if the drives are physically stolen.

Encrypting a Shared Folder

**Note**

- Default shared folders cannot be encrypted.
- The volume or path of an encrypted folder cannot be changed.
- Encrypted folders cannot be accessed through NFS.
- Shared folders on an encrypted volume cannot be encrypted. For details, see [Volumes](#).

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Locate a shared folder.
3. Under **Action**, click .
The **Edit Properties** window appears.
4. Select **Encrypt this folder**.
5. Specify the following information.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " \$: = \ This field does not support multibyte characters.
Verify Password	The password must match the previously specified password.
Save encryption key	When enabled, QTS automatically unlocks the shared folder after the NAS restarts. When disabled, users must unlock the folder after restarting the NAS. For details, see Unlocking a Shared Folder  Note QNAP strongly recommends exporting and saving the encryption key. For details, see Managing Encrypted Shared Folders.

The **Folder Encryption** window appears.

6. Review the information.

7. Click **Yes**.

Managing Encrypted Shared Folders

1. Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
2. Locate an encrypted shared folder.
3. Under **Action**, click .
The **Encryption Management** window appears.



Note

If the encrypted folder is locked, you must unlock it before configuring encryption settings. For details, see [Unlocking a Shared Folder](#).

4. Perform any of the following tasks.

Task	User Action
Download the encryption key file	a. Go to Download. b. Enter the encryption password. c. Click OK. QTS exports the encryption key file to your computer as a TXT.
Save the encryption key	a. Go to Save. b. Select Mount automatically on start up. When enabled, QTS automatically unlocks the shared folder after the NAS restarts. c. Enter the encryption password. d. Click OK. QTS saves the settings.  Tip Users can also save the encryption key when encrypting the shared folder. For details, see Encrypting a Shared Folder and Editing Shared Folder Properties.

Task	User Action
Lock the shared folder	a. Go to Lock. b. Optional: Select Forget the saved key.  Note When selected, users must unlock the folder after restarting the NAS. This setting is only available if Save encryption key was enabled when the folder was encrypted or Mount automatically on start up was enabled after the folder was encrypted. c. Click OK. QTS saves the changes.  Note - Locked folders do not appear in File Station. A folder will only reappear after it is unlocked. - Users cannot edit the properties or permissions of a locked shared folder.

Unlocking a Shared Folder

- Go to **Control Panel > Privilege > Shared Folders > Shared Folder**.
- Locate a locked shared folder.
- Under **Action**, click .
The **Unlock Folder** window appears.
- Select one of the following options.

Option	User Action
Input Encryption Password	a. Enter the encryption password. b. Optional: Select Save encryption key. When enabled, QTS automatically unlocks the shared folder after the NAS restarts.  Note This option is selected by default.
Upload Encryption Key File	a. Click Browse. b. Select the encryption key file.

- Click **OK**.

Quota

To efficiently allocate storage space, you can specify a quota value (in MB or GB) that applies to all users. When quotas are enabled, QTS prevents users from uploading data to the NAS after the quota is reached. By default, no quotas are set for the users.

You can also export quota settings to a CSV file after configuring them and then use the exported settings to review the quota allocated for each user or as a reference when configuring user accounts on other devices.

Configuring Quota Settings

1. Go to **Control Panel > Privilege > Quota** .
2. Select **Enable quota for all users**.
3. Specify the quota for all users.



Note

The quota must be between 100 MB and 2048 GB (2048000 MB).

4. Click **Apply**.
QTS displays the quota settings for each user.

Editing Quota Settings

1. Go to **Control Panel > Privilege > Quota** .
2. Select a volume.
3. Select a user.



Tip

By default, the **Quota** screen displays Local Users. To view domain users, select **Domain Users** in the drop-down menu on the right.

4. Click **Edit**.
The **Quota** window appears.
5. Specify a quota for the user.
6. Click **OK**.

Exporting Quota Settings

1. Go to **Control Panel > Privilege > Quota** .
2. Click **Generate**.
3. Click **Download**.

QTS exports the quota settings as a CSV file.

Domain Security

The NAS supports user authentication through local access rights management, the Microsoft Active Directory (AD), and the Lightweight Directory Access Protocol (LDAP) directory.

Joining the NAS to an AD domain or an LDAP directory allows AD or LDAP users to access the NAS using their own accounts without having to configure user accounts on the NAS.



Note

QTS supports AD running on Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, and 2016.

Go to **Control Panel > Privilege > Domain Security** to configure domain security settings.

Option	Description
No domain security (Local users only)	Only local users can access the NAS.
Active Directory authentication (Domain member)	Users can join the NAS to an AD, allowing domain users to be authenticated by the NAS. Local and AD users can access the NAS using Samba, AFP, FTP, and File Station. For details, see Active Directory (AD) Authentication .
LDAP authentication	Users can connect the NAS to an LDAP directory, allowing LDAP users to be authenticated by the NAS. Local and LDAP users can access the NAS using Samba, AFP, FTP, and File Station. For details, see LDAP Authentication .
Set this NAS as a domain controller	Clicking this directs the user to the Domain Controller screen. For details, see Domain Controller .

Active Directory (AD) Authentication

Active Directory (AD) is a Microsoft directory service that stores information for users, user groups, and computers for authenticating and managing domain access. Windows environments use AD to store, share, and manage a network's information and resources.

When a NAS is joined to an AD domain, the NAS automatically imports all of the user accounts on the AD server. AD users can then use the same login details to access the NAS.

Configuring AD Authentication Using the Quick Configuration Wizard

1. Go to **Control Panel > Privilege > Domain Security**.
2. Select **Active Directory authentication (Domain member)**.
3. Click **Quick Configuration Wizard**.
The **Active Directory Wizard** appears.
4. Click **Next**.
5. Specify the fully qualified domain name (FQDN) of the AD DNS server.
QTS automatically generates the **NetBIOS domain name**.
6. Specify the IP address of the AD DNS server.
7. Optional: Select **Obtain DNS server address automatically by DHCP server**.
8. Click **Next**.
9. Select a domain controller.
10. Specify the domain administrator username and password.
11. Click **Join**.
The NAS joins the domain.
12. Click **Finish**.

Configuring AD Authentication Manually

Verify the following before starting this task:

- The time settings of the NAS and the AD server are identical. The maximum time disparity tolerated is 5 minutes. For details, see [Configuring Time Settings](#).
- The AD server is configured as the primary DNS server. If you use an external DNS server, you will not be able to join the domain. For details, see [Network & Virtual Switch](#).
- You have specified the IP address of the WINS server that you use for name resolution. For details, see [Configuring Microsoft Networking](#).

1. Go to **Control Panel > Privilege > Domain Security**.
2. Select **Active Directory authentication (Domain member)**.
3. Click **Manual Configuration**.
The **Active Directory** window appears.
4. Specify the following information.

- **Domain NetBIOS Name**
- **AD Server Name**
- **Domain**
- **Domain Administrator Username**



Note

The specified user must have administrator access rights to the AD domain.

- **Domain Administrator Password**
- **Organizational Unit (Optional)**
- **Server description (Optional)**



Note

The NAS Samba service replicates this in the server's **Comment** field. This description appears when connecting to a NAS Samba shared folder using the command line interface.

5. Click **Join**.

AD Server and Domain Names

After joining the NAS to the AD domain, you can use the following username formats to log in to the NAS and access shared folders:

- **Local users:** NASname\NASusername
- **AD users:** Domain\DomainUsername

The location of AD server and domain names depends on the version of Windows Server.

Windows Server Version	Location
2003	Go to System Properties in Windows. Example: If the computer name is "node1.qnap-test.com", the AD server name is "node1" and the domain name is "qnap-test.com".
2008	Go to Control Panel > System in Windows. The AD server name will appear as the computer name, and the domain name can be found in the domain field.
2012, 2016	 Right-click  , and then click System . The AD server name will appear as the computer name, and the domain name can be found in the domain field.

Enabling Trusted Domain Authentication

A trusted domain is a domain that AD trusts to authenticate users. If you join the NAS to an AD domain, all users from trusted domains can log in and access shared folders.

Trusted domains are configured in AD. You can only enable trusted domains on the NAS. By default, this feature is disabled in QTS.

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > Microsoft Networking**.
2. Click **Advanced Options**.
The **Advanced Options** window appears.
3. Select **Enable trusted domains**.



Note

This setting is only available if the NAS is joined to a domain.

4. Click **Apply**.
The **Advanced Options** window closes.
5. Click **Apply**.

LDAP Authentication

A Lightweight Directory Access Protocol (LDAP) directory contains user and user group information stored on an LDAP server. Administrators can use LDAP to manage users in the LDAP directory and connect to multiple NAS devices with the same login details. This feature requires a running LDAP server and knowledge of Linux servers, LDAP servers, and Samba.

Configuring LDAP Authentication

1. Go to **Control Panel > Privilege > Domain Security**.
2. Select **LDAP authentication**.
3. Select the type of LDAP server.
4. Specify the following information.

LDAP Server Type	Fields	User Action
Remote LDAP server	LDAP Server Host	Specify the host name or IP address of the LDAP server.
	LDAP Security	Select the method that the NAS uses to communicate with the LDAP server. • ldap://: Use a standard LDAP connection. The default port is 389. • ldap:// (ldap + TLS): Use an encrypted connection with TLS. The default port is 389. Newer versions of LDAP servers normally use this port. • ldap:// (ldap + SSL): Use an encrypted connection with SSL. The default port is 686. Older versions of LDAP servers normally use this port.
	Base DN	Specify the LDAP domain. Example: <code>dc=mydomain,dc=local</code>
	Root DN	Specify the LDAP root user. Example: <code>cn=admin, dc=mydomain,dc=local</code>
	Password	Specify the root user password.
	Users Base DN	Specify the Organizational unit (OU) where users are stored. Example: <code>ou=people,dc=mydomain,dc=local</code>
	Group Base DN	Specify the OU where groups are stored. Example: <code>ou=group,dc=mydomain,dc=local</code>
	Current Samba ID	N/A
LDAP server of the remote NAS	IP address or NAS name	Specify the server IP address or the name of the NAS.
	LDAP domain	Specify the LDAP domain name.
	Password	Specify the NAS administrator password.
LDAP server of the local NAS	N/A	N/A
IBM Lotus Domino	This server type includes the same fields as Remote LDAP server , in addition to the following:	
	uidNumber	Specify the uid number. Select HASH .
	gidNumber	Specify the gid number. Select HASH .

- Click **Apply**.
The **LDAP authentication options** window appears.

- Select which users are allowed to access the NAS.


Note

LDAP authentication options vary depending on when Microsoft Networking is enabled. For details, see [LDAP Authentication Options](#).

- Click **Finish**.

LDAP Authentication Options

The **LDAP authentication options** vary depending on when Microsoft Networking is enabled.

For details, see [Microsoft Networking](#).

Scenario	Options
Microsoft Networking is enabled before LDAP settings are applied.	• Local users only: Only local users can access the NAS using Microsoft Networking. • LDAP users only: Only LDAP users can access the NAS using Microsoft Networking.
Microsoft Networking is enabled after the NAS is connected to the LDAP server.	• Standalone Server: Only local users can access the NAS using Microsoft Networking. • LDAP Domain Authentication: Only LDAP users can access the NAS using Microsoft Networking.

AD and LDAP Management

The administrator can modify domain user accounts and user groups when the NAS joins an AD domain or connects to an LDAP server.

Managing AD and LDAP Users

1. Go to **Privilege > Users**.
2. Select **Domain Users**.
QTS displays the list of domain users.
3. Locate a user.
4. Perform any of the following tasks.

Task	User Action
Edit an account profile	- Under Action, click . The Edit Account Profile window appears. - Edit the user quota.  Note User quotas must be enabled for this option to appear. For details, see Configuring Quota Settings.
Edit shared folder permissions	- Under Action, click . The Edit Shared Folder Permission window appears. - Edit the user's permissions for each shared folder. For details, see Shared Folder Permissions.

Task	User Action
Edit application privileges	a. Under Action, click . The Edit Application Privileges window appears. b. Select the applications that the user is allowed to access.  Tip QNAP recommends denying access to applications and network services that the user does not require. By default, administrator accounts have access to all applications.

**Tip**

Click  to display newly created users on the AD or LDAP server. Permission settings are automatically synchronized with the domain controller.

- Click **Apply**.

Managing AD and LDAP User Groups

- Go to **Control Panel > Privilege > User Groups**.
- Select **Domain Groups**.
QTS displays the list of domain user groups.
- Locate a user group.
- Perform any of the following tasks.

Task	User Action
View group details	Under Action, click . The View Group Details window appears. QTS displays the group name and group users.
Edit shared folder permissions	a. Under Action, click . The Edit Shared Folder Permission window appears. b. Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions.

**Tip**

Click  to display newly created groups on the AD or LDAP server. Permission settings are automatically synchronized with the domain controller.

- Click **Apply**.

Domain Controller

You can configure your QNAP NAS as a domain controller for Microsoft Windows environments. By configuring the NAS as a domain controller, you can store user account information, manage user authentication, and enforce security for a Windows domain.

Enabling a Domain Controller



Important

When the NAS is configured as a domain controller, only domain users can access shared folders through CIFS/SMB (Microsoft Networking). All local NAS users are denied access.

1. Go to **Control Panel > Privilege > Domain Controller**.
2. Select **Enable Domain Controller**.



Important

The domain controller cannot be enabled if an LDAP server is already running on the NAS.

3. Select the domain controller mode.

Mode	Description
Domain Controller	Only a domain controller can create a domain. The first NAS that creates the domain must be a domain controller. In this mode, the NAS can create and authenticate users.
Additional Domain Controller	If more than one domain controller is needed, you can add additional domain controllers. When the NAS is set as an additional domain controller, it can create and authenticate users.
Read-Only Domain Controller	This configures the NAS as a read-only domain controller to accelerate the user authentication process for specified websites. Read-only domain controllers can authenticate users, but not create domain user accounts.

4. Specify the following information.

Domain Controller Mode	Field	Description
Domain Controller	Domain	Specify the domain.
	Administrator Password	Specify an administrator password between 8 and 127 characters that contains at least one of each of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#\$%^&* _-+=` \'{}[];'"<>.,?/
	Verify Password	Verify the administrator password.
• Additional Domain Controller • Read-Only Domain Controller	Domain	Specify the domain.
	Domain DNS IP	Specify the domain DNS IP.
	Administrator Account	Specify the administrator account name.
	Administrator Password	Specify the administrator password.

5. Click **Apply**.

Resetting a Domain Controller

1. Go to **Control Panel > Privilege > Domain Controller** .
2. Click **Reset**.
A dialog box appears.
3. Enter the administrator password.
4. Click **OK**.

Default Domain User Accounts

Domain User Account	Description
Administrator	This account is used to configure settings, create users, and manage the domain. This account cannot be deleted.
Guest	Users without dedicated accounts can use this account to view and modify files.
krbtgt	This is the Key Distribution Center (KDC) service account. The KDC is a domain service that uses the Active Directory (AD) as the account database and the Global Catalog for directing referrals to KDCs in other domains.

Creating a Domain User

1. Go to **Control Panel > Privilege > Domain Controller > Users** .
2. Click **Create > Create a User** .
The **Create a User** wizard appears.
3. Click **Next**.
4. Specify the following information.

Field	Description
Username	Specify a username between 1 and 20 characters that does not: • Begin with a space • Begin with the following characters: - # @ • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' `
Password	Specify a password between 8 and 127 characters that contains at least three of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#\$%^&* _-+=` ()\} []:;'"<>,.?/
Description (optional)	Specify a user description that contains a maximum of 1024 ASCII characters.
Email (optional)	Specify an email address that will receive notifications from QTS. For details, see Email Notifications .

5. Click **Next**.
6. Specify the following information.

Setting	Description
User must change the password at first logon	The user must change the password after logging in for the first time.
Account expiration	Set an expiration date for the account. • Now: The account expires upon creation. • Expiry date: Specify an expiration date for the account.

7. Click **Next**.
8. Assign the account to existing Windows user groups.
9. Click **Next**.
10. Review the summary, and then click **Finish**.

Creating Multiple Domain Users

1. Go to **Control Panel > Privilege > Domain Controller > Users**.
2. Click **Create > Create Multiple Users**.
The **Create Multiple Users** wizard appears.
3. Click **Next**.
4. Specify the following information.

Field	Description
User Name Prefix	Specify a username prefix between 1 and 16 ASCII characters that does not: • Begin with a space • Begin with the following characters: - # @ • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' . This prefix will be included before all usernames.
User Name Start No	Specify a starting number up to 8 digits in length.  Note QTS removes leading zeros in starting numbers. For example, 001 becomes 1.
Number of Users	Specify a number between 1 and 4095. This number signifies the number of accounts that will be created.

Field	Description
Password	Specify a password between 8 and 127 characters that contains at least three of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#\$%^&* _-+=` \\(){} []:;'"<>,.?/
User must change the password at first logon	The user must change the password after logging in for the first time.
Account expiration	Set an expiration date for the account. • Now: The account expires upon creation. • Expiry date: Specify an expiration date for the account.

- Click **Create**.
QTS creates the accounts and adds them to the list of domain users.
- Click **Finish**.

Domain User Account Lists

User accounts can also be imported directly from TXT or CSV files. The files contain user account information including usernames, passwords, descriptions, and email addresses.

File Format	Description
TXT	Create domain user account lists using a text editor. For details, see Creating a TXT Domain User File .
CSV	Create domain user account lists using a spreadsheet editor. For details, see Creating a CSV Domain User File .

Creating a TXT Domain User File

- Create a new file in a text editor.
- Specify domain user information in the following format.
Username,Password,Description,Email



Important

- Separate values using commas.
- Ensure that the password meets the requirements for domain user accounts. For details, see [Creating a Domain User](#).

- Specify information for only one user on each line.
Example:

```
John,s8fK4br*,John's account,john@qnap.com
Jane,9fjwbXy#,Jane's account,jane@qnap.com
Mary,f9xn3nS%,Mary's account,mary@qnap.com
```

3. Save the list as a TXT file.



Important

If the list contains multi-byte characters, save the file with UTF-8 encoding.

Creating a CSV Domain User File

1. Create a new workbook in a spreadsheet editor.
2. Specify domain user information in the following format.

- column A: Username
- column B: Password
- column C: Description
- column D: Email



Important

- Ensure that the password meets the requirements for domain user accounts. For details, see [Creating a Domain User](#).
- Specify information for only one user in each row.
Example:

	A	B	C	D
1	John	s8fK4b*	John's account	john@qnap.com
2	Jane	9fjwbX#	Jane's account	jane@qnap.com
3	Mary	f9xn3nS%	Mary's account	mary@qnap.com

3. Save the workbook as a CSV file.



Important

If the list contains multi-byte characters, open the file using a text editor and then save with UTF-8 encoding.

Batch Importing Domain Users

1. Go to **Control Panel > Privilege > Domain Controller > Users**.
2. Click **Create > Batch Import Users**.
The **Batch Import Users** wizard appears.
3. Optional: Select **Overwrite existing users**.



Important

When selected, QTS overwrites existing domain user accounts that have duplicates on the imported domain user account list.

4. Click **Browse**, and then select the file that contains the domain user account list.

**Important**

Ensure that you are importing a valid QTS domain user account list file to avoid parsing errors.

For details, see [Domain User Account Lists](#).

5. Click **Next**.

The **File content preview** screen appears.

**Important**

Ensure that the file contents are valid. If any information is invalid, the domain user account list cannot be imported.

6. Click **Import**.

QTS imports the domain user account list.

7. Click **Finish**.

Modifying Domain User Account Information

1. Go to **Control Panel > Privilege > Domain Controller > Users**.

2. Locate a user.

3. Perform any of the following tasks.

Task	User Action
Change password	a. Under Action, click . The Change Password window appears. b. Specify a password that meets the requirements. c. Verify the password. d. Click Change.
Edit user properties	a. Under Action, click . The Edit User Properties window appears. b. Edit the user properties. For details, see Creating a Domain User. c. Click Finish.
Edit user group membership	a. Under Action, click . The Edit User Groups wizard appears. b. Select or deselect user groups. For details, see Domain User Groups. c. Click Next. d. Review the summary, and then click Finish.

Task	User Action
Edit user profile	a. Under Action, click . The Edit User Profile window appears. b. Specify the following: • Profile path Specify the shared folder where the roaming profiles are stored. • Login script Specify the login script that executes when a domain user logs in from a computer member of the domain. To directly specify the script filename, connect to \\NAS\\netlogon using the domain administrator account and copy the script to the /sysvol shared folder in the \\scripts folder of your domain. • Home Folder Specify the drive and shared folder that is mapped to the drive when the domain user logs in to the domain. • Click Finish.

**Tip**

You can also edit quota settings for domain users. For details, see [Editing Quota Settings](#).

Deleting Domain Users

1. Go to **Control Panel > Privilege > Domain Controller > Users**.
2. Select the domain users to delete.

**Note**

The administrator account cannot be deleted.

3. Click **Delete**.
A warning message appears.
4. Click **Yes**.

Domain User Groups

A domain user group is a collection of domain users with the same access rights to files and folders. Domain administrators can create domain user groups to improve security for domain users.

Default Domain User Groups

- Allowed RODC Password Replication Group
- Certificate Service DCOM Access
- Denied RODC Password Replication Group
- Enterprise Read-Only Domain Controllers
- Incoming Forest Trust Builders

- Network Configuration Operators
- Pre-Windows 2000 Compatible Access
- Read-Only Domain Controllers
- Terminal Server License Servers
- Windows Authorization Access Group

Creating a Domain User Group

1. Go to **Control Panel > Privilege > Domain Controller > Groups** .
2. Click **Create a User Group**.
The **Create a User Group** wizard appears.
3. Specify a user group name between 1 and 128 ASCII characters that does not begin with:
 - Spaces
 - The following characters: - # @
4. Click **Next**.
5. Optional: Add users to the group.
 - a. Select **Yes**.
 - b. Click **Next**.
 - c. Select the users you want to add to the group.
 - d. Click **Next**.
6. Review the summary, and then click **Finish**.

Editing Domain User Groups

1. Go to **Control Panel > Privilege > Domain Controller > Groups** .
2. Locate a domain user group.
3. Under **Action**, click  .
The **Edit Group Users** wizard appears.
4. Select or deselect user groups.
5. Click **Next**.
6. Review the summary, and then click **Finish**.

Deleting Domain User Groups

1. Go to **Control Panel > Privilege > Domain Controller > Groups** .
2. Select the user groups to delete.

**Note**

Some default user groups cannot be deleted.

**Important**

Do not delete the default group of the domain.

3. Click **Delete**.
A warning message appears.
4. Click **Yes**.

Computers

The **Computers** screen displays the computer accounts for computers or NAS devices that have joined the domain. Computer accounts are created automatically when a computer or NAS joins the domain.

Creating a Computer Account

1. Go to **Control Panel > Privilege > Domain Controller > Computers**.
2. Click **Create a Computer**.
The **Create a Computer** wizard appears.
3. Specify the following information.

Field	Description
Computer name	Specify a computer name between 1 and 15 ASCII characters that include any of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Dashes (-)
Description	Specify a user description that contains a maximum of 1024 ASCII characters.
Location	Specify the location of the computer using a maximum of 1024 ASCII characters.

4. Click **Next**.
5. Assign the account to existing Windows user groups.
6. Click **Next**.
7. Review the summary, and then click **Create**.

Modifying Computer Account Information

1. Go to **Control Panel > Privilege > Domain Controller > Computers**.
2. Locate a computer account.
3. Perform any of the following tasks.

Task	User Action
Edit computer properties	- Under Action, click . The Edit computer properties window appears. - Edit the Description or Location. For details, see Creating a Computer Account.
Edit user group membership	- Under Action, click . The Edit User Groups window appears. - Select or deselect user groups. For details, see Domain User Groups. - Click Next.

- Click **Finish**.

Editing Computer Account Shared Folder Permissions

- Go to **Control Panel > Privilege > Computers**.
- Locate a computer account.
- Under **Action**, click . The **Edit Shared Folder Permission** window appears.
- Edit the computer account's permissions for each shared folder. For details, see [Shared Folder Permissions](#).
- Click **Apply**.

Deleting Computer Accounts

- Go to **Control Panel > Privilege > Domain Controller > Computers**.
- Select the accounts to delete.



Note

The host computer account cannot be deleted.

- Click **Delete**. A warning message appears.
- Click **Yes**.

DNS

The Domain Name System (DNS) helps the domain controller locate services and devices within the domain using service and resource records. Two DNS zones are created by default: the domain created when setting up the NAS as a domain controller, and a zone called "_msdcs". System administrators can modify DNS settings and add or delete domains and records.

Modifying DNS Settings

- Go to **Control Panel > Privilege > Domain Controller > DNS**.

2. Log in under the domain administrator account.


Note

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

3. Under **DNS Settings**, select a domain.
A list of records appears.
4. Select a record.
The properties panel appears.
5. Modify any of the following.

Field	Description
Name	Edit the name of the record.
Type	Select the type of record.

6. Modify the values.

Task	User Action
Add a value	a. Specify a value. b.  Click . The value is added to the list.
Move a value up	a. Select a value from the list. b.  Click . The value moves up in the list.
Move a value down	a. Select a value from the list. b.  Click . The value moves down in the list.
Remove a value	a. Select a value from the list. b.  Click . The value is removed from the list.

7. Click **Apply**.

Adding Domains

1. Go to **Control Panel > Privilege > Domain Controller > DNS**.

2. Log in under the domain administrator account.

**Note**

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

3. Click **Action > Add Domain** .
The **Add New Domain** window appears.
4. Enter the domain name.
5. Click **Create**.

Adding Records

1. Go to **Control Panel > Privilege > Domain Controller > DNS** .
2. Log in under the domain administrator account.

**Note**

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

3. Select a domain or record.
4. Click **Action > Add Record** .
The **Add New Record** window appears.
5. Specify the following information.

Field	Description
Record Name	Specify the name of the record.
Type	Select the type of record.
Value	Specify the value.

6. Click **Create**.

Deleting Domains or Records

1. Go to **Control Panel > Privilege > Domain Controller > DNS**.
2. Log in under the domain administrator account.



Note

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

3. Select a domain or record to delete.
4. Click **Action > Delete**.
A warning message appears.
5. Click **Yes**.

Back Up/Restore

Users can back up or restore domain controller settings. Only the primary domain controller needs to be backed up; backing up the primary domain controller also backs up any additional or read-only domain controllers. When restoring a domain controller, there are some restrictions and limitations if the domain controller is in an AD environment with more than one domain controller. For details, see [Restoring Domain Controllers](#).

Backing Up Domain Controllers

1. Go to **Control Panel > Privilege > Domain Controller > Backup/Restore**.
2. Under **Back up ADDC Database**, select **Back up Database**.
3. Specify the following information.

Option	Description
Backup frequency	Select how often the Active Directory Domain Controller (ADDC) database is backed up.
Start Time	Select when the backup will begin.
Destination folder	Select the NAS folder where the backup will be stored.
Backup Options	Select one of the following: • Overwrite existing backup file (dc_backup.exp) • Create a new file for each backup and append the date to the filename (dc_backupyyyy_mm_dd_exp)

4. Click **Apply**.

Restoring Domain Controllers



Important

Restoring a domain controller overwrites all user, user group, and domain controller settings. Any changes made after the backup file was created will be lost.



Warning

Restoring a domain controller in a multiple-controller environment from a backup file will corrupt the domain controller database. Instead, re-add the NAS as a domain controller, and it will synchronize with the existing controller.

1. Go to **Control Panel > Privilege > Domain Controller > Backup/Restore** .
2. Under **Restore ADDC Database**, click **Browse**.
3. Locate a domain controller backup file.
4. Click **Import**.

6. Network & Virtual Switch

About Network & Virtual Switch

Network & Virtual Switch is a QTS utility that centralizes the creation, configuration, and control of network connections. Network & Virtual Switch also manages physical network interfaces, virtual adapters, Wi-Fi, and Thunderbolt connections in addition to controlling DHCP, DDNS, and gateway services.

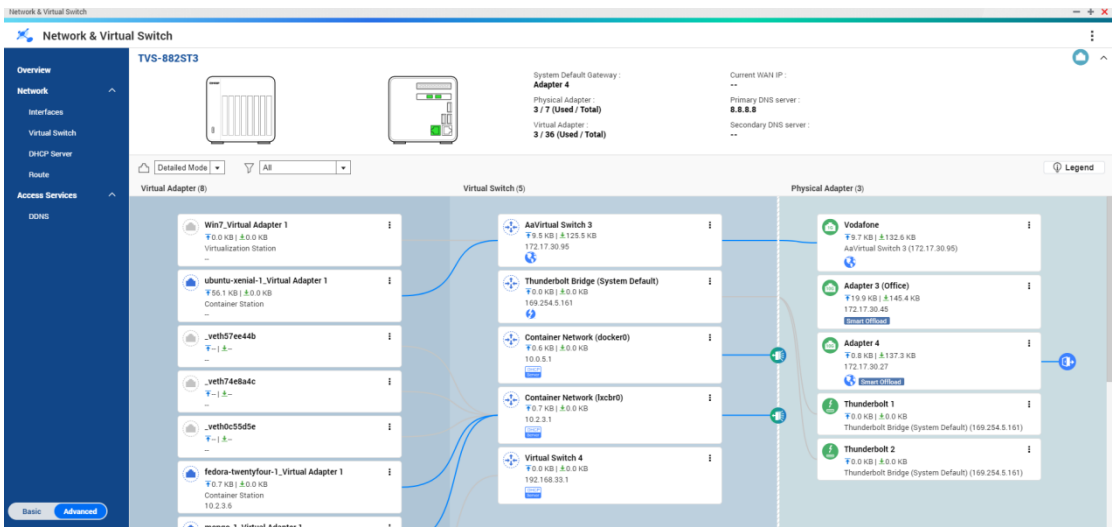
Basic and Advanced Mode

Network & Virtual Switch features two separate usage modes. Switch between these modes by clicking **Basic** or **Advanced** in the Network & Virtual Switch menu pane.

Mode	Description
Basic	This mode is well-suited for most users, and requires minimal configuration of network settings. - Virtual Switch functions are disabled. - Static Route functions are disabled.
Advanced	This mode is best-suited for power-users who need more control over the configuration of network settings. - Virtual Switch functions are enabled. - Static Route functions are enabled.

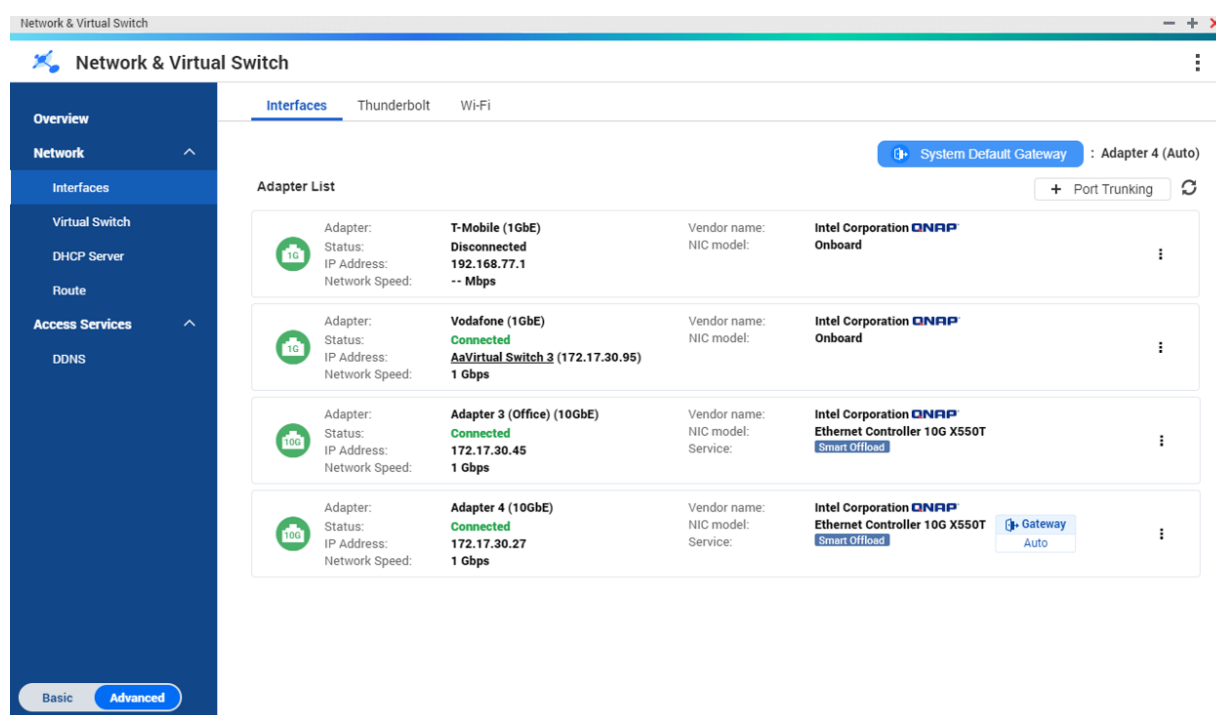
Overview

This screen provides a general overview of the network topology, IP address, status, and usage information for each device on the network.



Interfaces

This screen provides access to basic network settings and allows the configuration of physical adapters. This screen also contains settings related to IPv4, IPv6, DNS, port trunking, VLAN, Thunderbolt, USB QuickAccess, and Wi-Fi.



IP Address

Configuring IPv4 Settings

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
4. Configure the IPv4 settings.

Setting	Description
Obtain IP address settings automatically via DHCP	If the network supports DHCP, the adapter automatically obtains the IP address and network settings.

Setting	Description
Use static IP address	Manually assign a static IP address. You must specify the following information: • Fixed IP Address • Subnet Mask • Default Gateway
Jumbo Frame	Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QTS supports the following MTU sizes: • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes  Important • All connected network devices must enable Jumbo Frames and use the same MTU size. • Only certain NAS models support Jumbo Frames. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster.
Network Speed	Select the network transfer rate allowed by the NAS network environment.  Tip Selecting Auto-negotiation will automatically detect and set the transfer rate.  Important The Network Speed field is automatically set to Auto-negotiation and hidden when configuring 10GbE & 40GbE adapters.

5. Click **Apply**.

Configuring IPv6 Settings

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .

3. Identify the adapter that you want to configure and then click  > **Configure** .
The **Configure** window opens.
4. Go to the **IPv6** tab.
5. Configure the IPv6 settings.

Setting	Description
Disable	Do not assign an IPv6 address.
IPv6 Auto-Configuration (Stateful)	The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.  Important This option requires an available DHCPv6-enabled server on the network.
IPv6 Auto-Configuration (Stateless)	The adapter automatically acquires an IPv6 address and DNS settings from the router.  Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network.
Use static IP address	Manually assign a static IP address to the adapter. You must specify the following information: - Fixed IP Address - Prefix length  Tip Obtain the prefix length information from your network administrator. - Default Gateway

6. Click **Apply**.

DNS

A Domain Name System (DNS) server translates a domain name into an IP address.

Configuring DNS Settings

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
4. Go to the **DNS** tab.

5. Select one of the following options:

Setting	Description
Obtain DNS server address automatically	Automatically obtain the IP address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

6. Click **Apply**.

Virtual LANs (VLANs)

A Virtual LAN (VLAN) is a group of hosts which communicate as if they were attached to the same broadcast domain even if they are in different locations. You can use VLANs to increase security and flexibility, while decreasing network latency and load.

Adding an Interface to a VLAN



Important

When using both port trunking and a VLAN, port trunking must be configured first.

- Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
- Go to **Network > Interfaces** .
- Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
- Go to the **VLAN** tab.

Setting	Description
Obtain DNS server address automatically	Automatically obtain the IP address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

5. Select **Enable VLAN**.

6. Specify a VLAN ID.



Important

- The VLAN ID must be between 1 and 4094.
- Make a note of the VLAN ID before completing this process. If the VLAN ID is lost, the network settings will need to be reset.

7. Click **Apply**.

Port Trunking

Port trunking combines two or more Ethernet interfaces for increased bandwidth, load balancing and fault tolerance (failover). Load balancing is a feature that distributes workloads evenly across multiple Ethernet interfaces for higher redundancy. Failover ensures that a network connection remains available even if a port fails.

Configuring Port Trunking



Important

Before configuring Port Trunking, ensure at least two network interfaces are connected to the same switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Click **Port Trunking**.
The **Port Trunking** window opens.
4. Click **Add**.
The **Port Trunking (Add)** window opens.
5. Select two or more network interfaces to add to the trunking group.
6. Click **Next**.
7. Select a switch type.
8. Click **Next**.
9. Select a trunking mode.



Important

Some port trunking modes must be supported by your network switches. Selecting an unsupported mode may affect network performance or cause the network interface to freeze.

Mode	Description
Fault Tolerance (Failover)	
Active-Backup	All traffic is sent and received using the interface that was first added to the trunking group. If this primary interface becomes unavailable, the secondary interface will become active.
Broadcast	Transmits the same network packets to all the network interface cards.
Load balancing & Failover	
Balance-tlb	Incoming traffic is received by the current interface. If the interface fails, a slave interface takes over the MAC address of the failed interface. Outgoing traffic is distributed based on the current load for each interface relative to the interface's maximum speed.
Balance-alb	Similar to Balance-tlb, but offers additional load balancing for incoming IPv4 traffic.
Balance-rr	Transmits network packets sequentially to each network interface card in order to distribute the internet traffic among all the NICs.

Mode	Description
Balance-xor	Transmits network packets using the Hash algorithm, which selects the same NIC slave for each destination MAC address.
802.3ad dynamic	Uses a complex algorithm to aggregate NICs and configure speed and duplex settings.

- Click **Apply**.

System Default Gateway

The system default gateway serves as the network access point for the NAS. By default, all external network traffic will pass through the gateway. A network interface must be specified for the default gateway.

Configuring the System Default Gateway

- Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
- Go to **Network > Interfaces** .
- Click **System Default Gateway**.
The **System Default Gateway** window opens.
- Configure the system default gateway.

Setting	Description
Auto-select system default gateway	QTS automatically detects all adapter, virtual switch, PPPoE, and VPN connections that can be used to connect to the internet. It selects one of these connections and then sets it as the default gateway.
Select the system default gateway	Manually assign an adapter to serve as the system default gateway. Optionally, set a backup failover gateway. The failover default gateway field is only available when multiple interfaces are connected.  Tip When assigning a PPPoE or VPN connection as the default gateway, ensure a stable physical connection is also set as the failover default gateway.

- Optional: Disable the NCSI service.



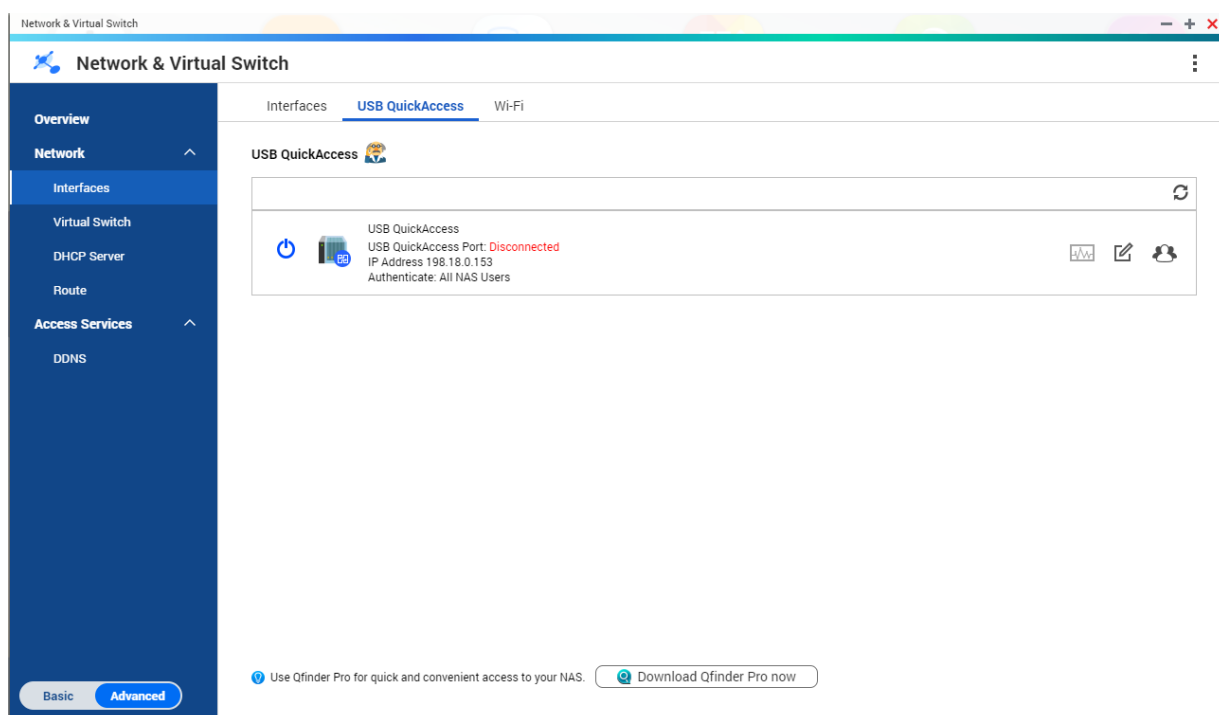
Tip

The QTS Network Connectivity Status Indicator (NCSI) periodically performs tests to check the speed and status of NAS network connections.

- Click **Apply**.

USB QuickAccess

This screen controls the configuration and management of USB QuickAccess services on the NAS. USB QuickAccess allows a computer to connect to the NAS using a USB cable and the Common Internet File System (CIFS).



Tip

- USB QuickAccess is only available on certain models.
- It is not possible to configure, delete, or disable DHCP servers created with USB QuickAccess.

Enabling USB QuickAccess

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4.  .
Click .

Configuring the USB QuickAccess IP address

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4.  .
Click .
The **Configure** window opens.

5. Enter a static IP Address.

6. Click **Apply**.

Configuring USB QuickAccess Authentication

1. Go to **Control Panel > Network & Virtual Switch** .

The **Network & Virtual Switch** window opens.

2. Go to **Network > Interfaces** .

3. Go to the **USB Quick Access** tab.

4.



Click

The **Configuration** window opens.

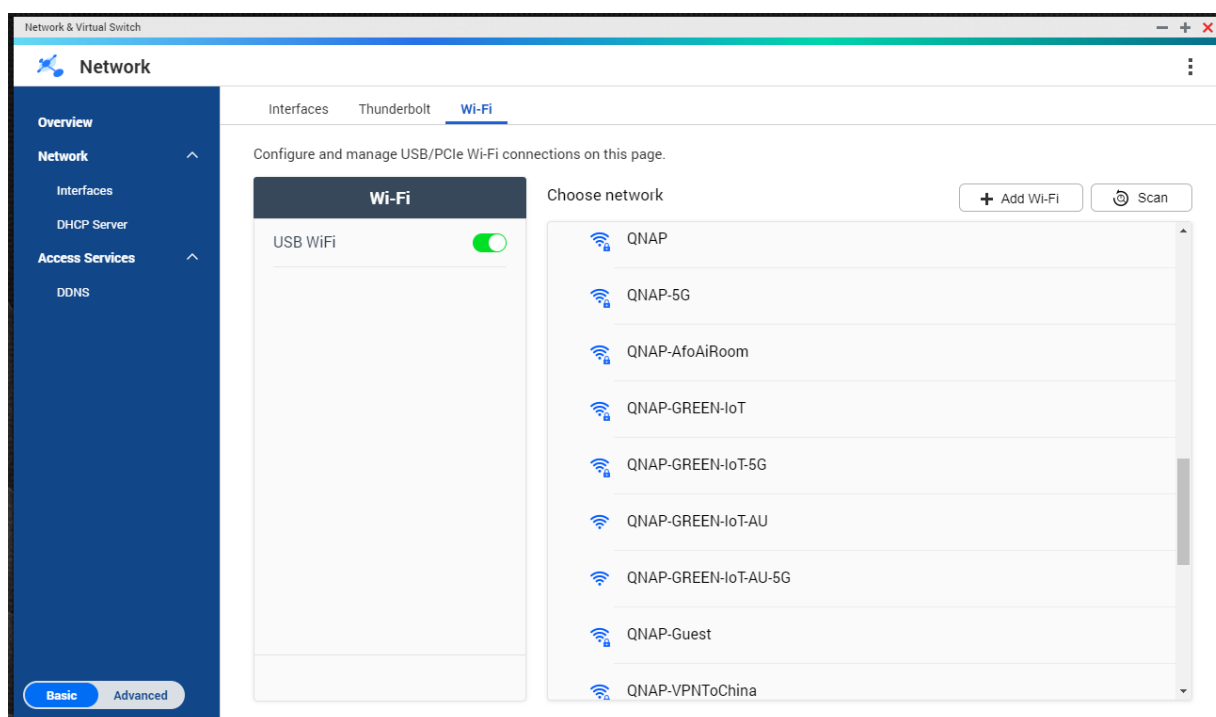
5. Select an authentication method:

Authentication Method	Description
All NAS Users	A QTS username and password is required to access files.
Everyone	No username or password is required to access files.
Selected Users/Groups	Administrators can grant access to specific QTS users or groups. A QTS username and password is required to access files.  Tip To grant access to domain users, first set up Domain Security. Go to Control Panel > Privilege > Domain Security .

6. Click **Apply**.

Wi-Fi

This screen controls the configuration and management of Wi-Fi connections accessible from the NAS.



Important

- A USB or PCIe Wi-Fi device must be installed to access these features.
 - For a list of compatible USB Wi-Fi dongles, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > USB Wi-Fi**.
 - For a list of compatible PCIe Wi-Fi cards, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > Expansion Card > QNAP**.
- QTS supports the simultaneous use of multiple PCIe Wi-Fi cards, but only one USB Wi-Fi dongle can be in used at a time.

Enabling Wi-Fi

1. Go to **Control Panel > Network & Virtual Switch**.
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces**.
3. Go to the **Wi-Fi** tab.
4. Click .

Connecting to a Wireless Network

1. Go to **Control Panel > Network & Virtual Switch**.
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces**.

3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible networks.
5. Select a wireless network from the list.

Icon	Description
	The Wi-Fi network requires a password.
	Connect to a Wi-Fi network without a password.
	• The Wi-Fi connection cannot access the internet. • The Wi-Fi connection requires an additional login.  Tip QTS does not support networks that require an additional login.

The settings panel expands.

6. Click **Connect**.
7. Optional: Configure connection settings.

Setting	Description
Password	Enter the password provided by the network administrator.  Tip Click  to make the password visible.
Connect automatically	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

8. Click **Apply**

Adding a Wireless Network

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Click **Add Wi-Fi**.
The **Connect to a Wi-Fi network** window opens.
5. Configure connection settings.

Setting	Description
Network Name	Enter the name of the wireless network.
Security Type	Select the encryption used by the wireless network.
Password	Enter the password provided by the network administrator.  Tip Click  to make the password visible.
Automatically connect when the	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

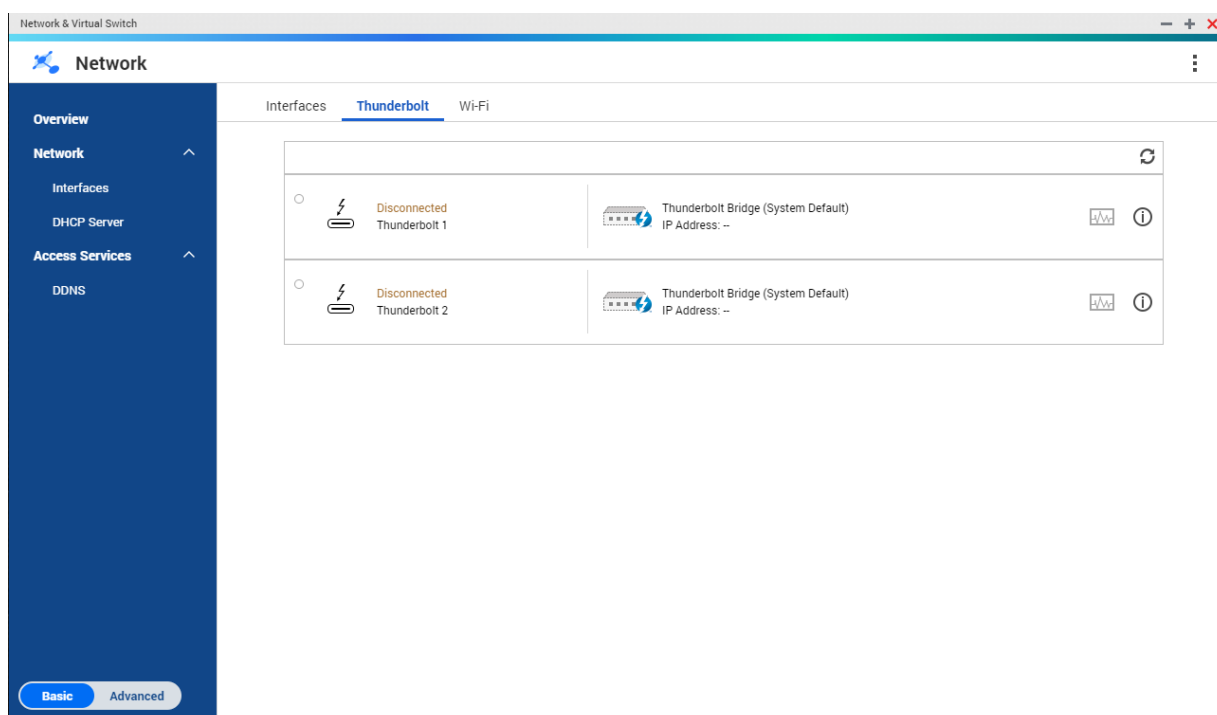
6. Click **Connect**.

Connection Messages

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

Thunderbolt

This screen displays port and connection information related to any Thunderbolt interfaces on the NAS.



Thunderbolt to Ethernet (T2E)

Thunderbolt to Ethernet functionality allows the Thunderbolt port to act as an Ethernet interface.



Tip

QNAP recommends using Qfinder Pro when configuring Thunderbolt to Ethernet.



Important

Due to Thunderbolt driver issues, T2E connections using Thunderbolt 2 may have connectivity problems when connecting to Windows. Thunderbolt 3 connections are unaffected.

Enabling T2E with Qfinder Pro

Qfinder Pro is a utility for Windows, Mac, and Linux that allows you to quickly find and access a QNAP NAS over a LAN.

For the current version of Qfinder Pro, please visit <https://www.qnap.com/utilities>.



Tip

Qfinder Pro automatically configures the `/etc/sysctl.conf` settings file on macOS.

1. Open **Qfinder Pro**.
2. Locate the NAS using **Qfinder Pro**.
3. Click the Thunderbolt icon.
The T2E window opens.
4. Select **Enable T2E**.
5. Click **Apply**.

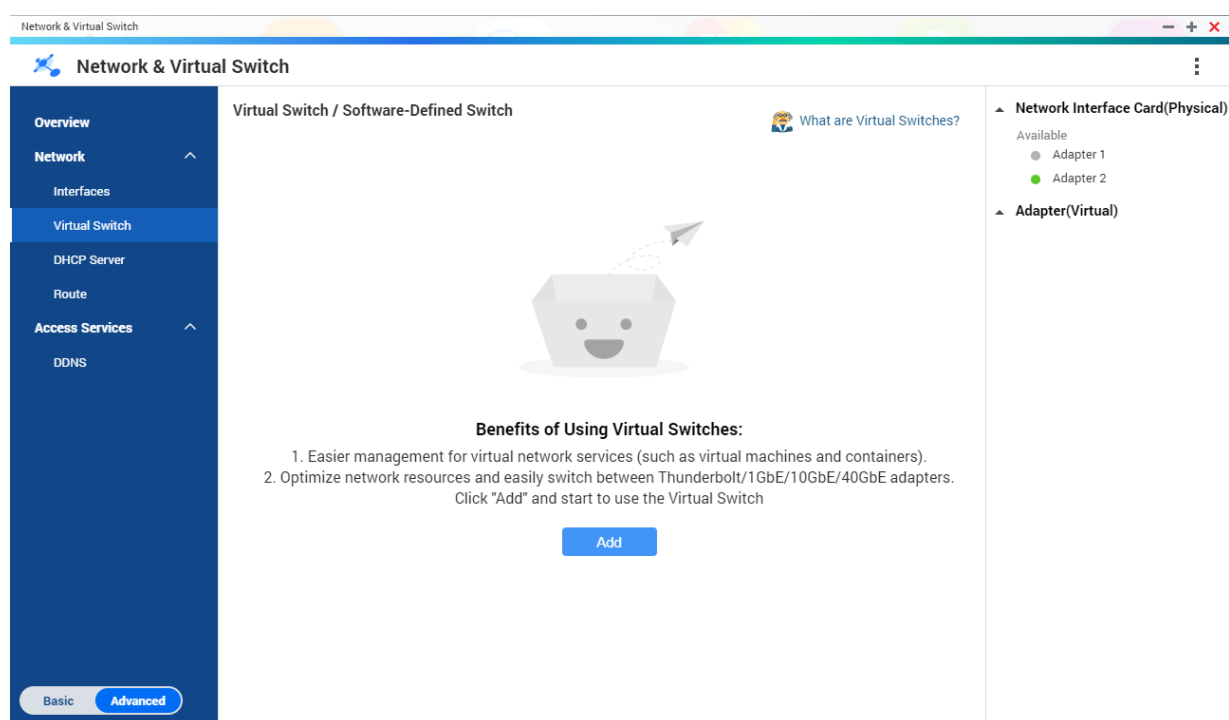
Enabling T2E on macOS

1. Open the Terminal.
2. Run the command.

Command	Notes
<code>sudo sysctl net.inet.tcp.path_mtu_discovery=0 && sudo sysctl net.inet.tcp.tso=0</code>	This command will only temporarily enable T2E. Restarting the Mac will delete the connection.
<code>sudo bash -c 'printf "#QNAP\nnet.inet.tcp.path_mtu_discovery=0\nnet.inet.tcp.tso=0\n#QNAP\n" >> /etc/sysctl.conf'</code>	This command will permanently apply these settings.

Virtual Switches

This screen controls the configuration and management of virtual switches running on the NAS. Virtual Switches allow physical interfaces and virtual adapters to communicate with each other.



QTS supports three different virtual switch modes.

Mode	Description
Basic	This mode is well-suited for most users, and requires minimal configuration of network settings.
Advanced	This mode is best-suited for power-users who need more control over the configuration of network settings.

Mode	Description
Software-Defined Switch	This mode is suited for power-users who need to simulate an L2 physical switch.  Important Packet forwarding rates are limited when using this mode.

**Tip**

To access this page, Network & Virtual Switch must be operating in [Advanced Mode](#).

Creating a Virtual Switch in Basic Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Basic Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Apply**.

Creating a Virtual Switch in Advanced Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Advanced Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Next**.
8. Configure the virtual switch IP address.

Address Type	Description
DHCP Client	Assigns a dynamic IP address to the virtual switch.
Static IP	Assigns a static IP address to the virtual switch.  Tip Examine your network setup for guidance on how to best configure these settings.
Do not assign IP Addresses	Does not assign an IP address to the virtual switch after creation.  Tip This setting should be used when creating a virtual switch for special purposes, such as when building an external or isolated network.

9. Click **Next**.

10. Configure the virtual switch services.

a. Enable the NAT service.



Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- The IP address of the virtual switch cannot be in a reserved range that doesn't support forwarding:
 - 127.xxx.xxx.xxx
 - 169.254..xxx.xxx
 - 192.0.2.xxx
 - 198.51.100.xxx
 - 203.0.113.xxx

b. Optional: Enable the DHCP Server.



Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- To avoid IP address conflicts, do not enable DHCP server if there is another DHCP server running on the local network.

Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.

Setting	Description
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.
WINS Server	Specify the WINS server IP address.  Tip Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server.  Tip QTS supports both PXE and remote booting of devices
Boot File	Specify location and file name of the TFTP server boot file.  Tip QTS supports both PXE and remote booting of devices

11. Click **Next**.

12. Configure the virtual switch IPv6 address.

Setting	Description
Disable	Do not assign an IPv6 address.

Setting	Description
IPv6 Auto-Configuration (Stateful)	The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.  Important This option requires an available DHCPv6-enabled server on the network.
IPv6 Auto-Configuration (Stateless)	The adapter automatically acquires an IPv6 address and DNS settings from the router.  Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network.
Use static IP address	Manually assign a static IP address. You must specify the following information: • Fixed IP Address • Prefix length  Tip Obtain the prefix length information from your network administrator. • Default Gateway

13. Click **Next**.

14. Configure the DNS settings.

Setting	Description
Obtain DNS server address automatically	Automatically obtain the DNS server address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

15. Click **Next**.

16. Confirm the virtual switch settings.

17. Click **Apply**.

Creating a Virtual Switch in Software-defined Switch Mode



Important

To avoid bridge loops, please ensure any Ethernet cables are connected to the same switch before configuring a Software-defined Switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch**.

The **Network & Virtual Switch** window opens.

2. Go to **Network > Virtual Switch**.
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Software-defined Switch Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.



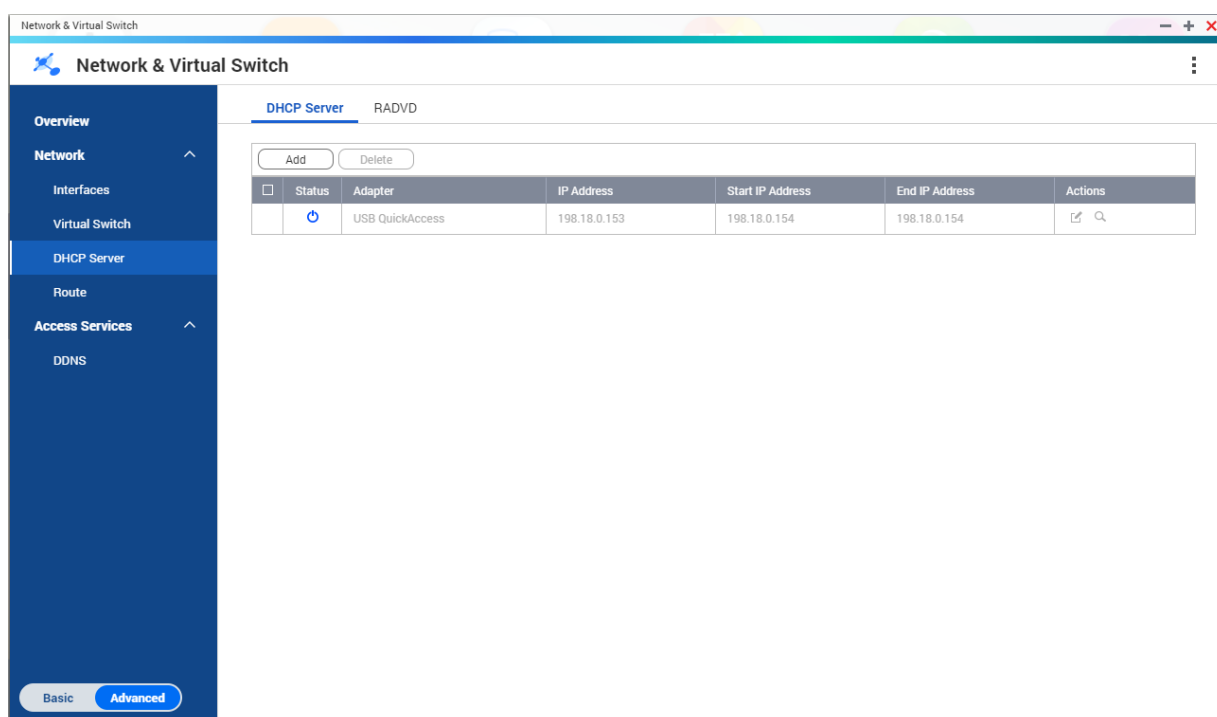
Tip

Enabling this setting prevents bridge loops.

7. Click **Apply**.

DHCP Server

This screen controls the creation and management of Dynamic Host Configuration Protocol (DHCP) servers. DHCP servers can assign IPv4 addresses to clients on the network, while RADVD servers assign IPv6 addresses.



Important

Do not create a new DHCP server if one already exists on the network. Enabling multiple DHCP servers on the same network can cause IP address conflicts or network access errors.

Creating a DHCP Server

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Click **Add**.
The **DHCP Server** window opens.
4. Select an interface.
5. Click **Next**.
6. Select the network environment for the DHCP server.

Option	Description
Enable DHCP server on the current network.	• The adapter keeps the existing IP address and subnet mask. • The DHCP server shares the subnet mask with the adapter and is assigned the next available IP address.
Reassign an IP address to the adapter and enable a DHCP server on a new subnet.	• The adapter is assigned a new IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.
Enable DHCP server for another subnet.	• The adapter keeps the existing IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.

7. Click **Next**.
8. Configure a static IP address for the adapter.



Important

A static IP address must be configured when creating a DHCP server.

- a. Click **Yes**.
- b. Configure IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address.  Tip Examine your network setup for guidance on how to best configure these settings.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.

Setting	Description
Default Gateway	Specify the IP address of the default gateway for the adapter.
Jumbo Frame	Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QTS supports the following Jumbo Frame sizes: • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes  Important • Jumbo Frames are only supported by certain NAS models. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster. All connected network devices must enable Jumbo Frames and use the same MTU size.
Network Speed	Specify the speed at which the adapter will operate.  Tip Auto-negotiation will automatically detect and set the transfer rate.
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	Assign an IP address for the secondary DNS server.
	 Important QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Next**.

9. Configure DHCP settings.

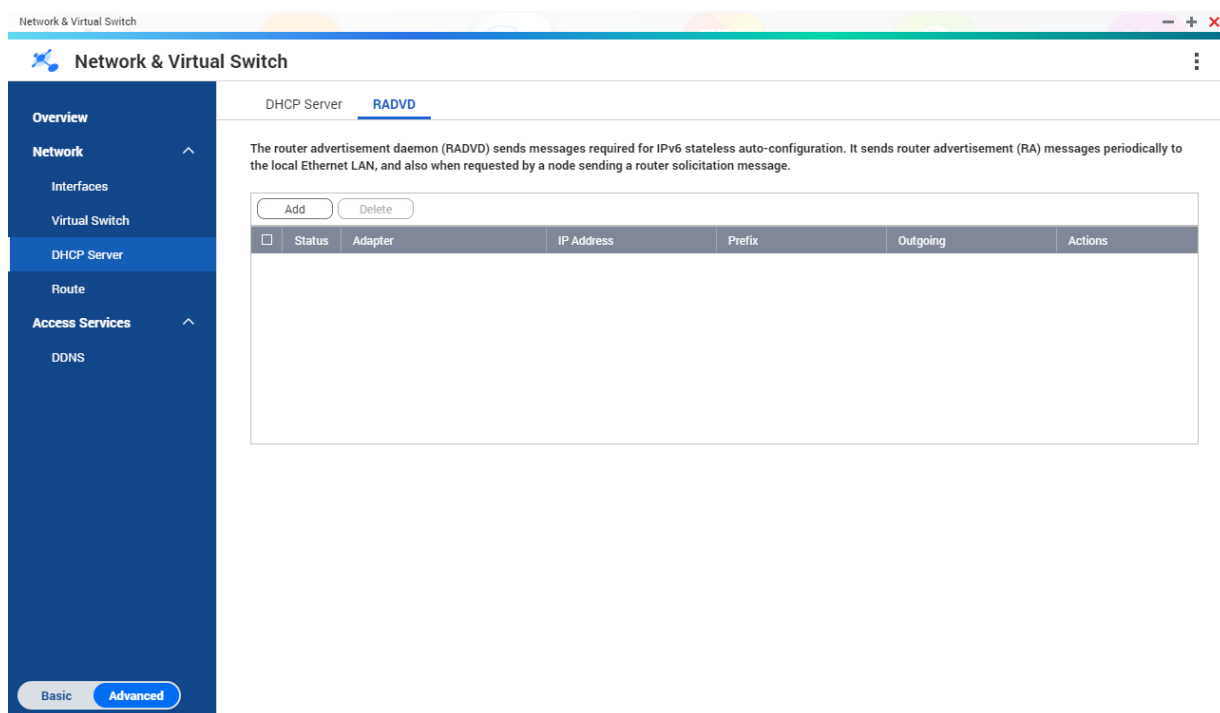
Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.

Setting	Description
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.
WINS Server	Specify the WINS server IP address.  Tip Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server.  Tip QTS supports both PXE and remote booting of devices
Boot File	Specify location and file name of the TFTP server boot file.  Tip QTS supports both PXE and remote booting of devices

10. Click **Apply**.

RADVD

This screen controls the creation and management of Router Advertisement Daemon (RADVD) servers. This service sends messages required for IPv6 stateless auto-configuration. This service periodically sends router advertisement (RA) messages to devices on the local network, and can also send a router solicitation messages when requested from a connected node.



Creating an RADVD Server

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Go to the **RADVD** tab.
4. Click **Add**.
The **RADVD - Outgoing Interface** window opens.
5. Select the outgoing interface.
6. Click **Next**.
7. Configure a static IP address for the adapter.



Important

A static IP address must be configured when creating a RADVD server.

- a. Click **Yes**.
- b. Optional: Configure Static IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address.
	 Tip Examine your network setup for guidance on how to best configure these settings.

Setting	Description
Prefix Length	Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	Assign an IP address for the secondary DNS server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Next**.

8. Select a second adapter for the RADVD service interface.

9. Click **Next**.

10. Optional: Configure a static IP address for the second RADVD adapter.



Important

Creating an RADVD interface requires that the adapter use a static IP address. If the adapter already uses a static IP address, skip this step.

a. Click **Yes**.

b. Configure Static IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address.  Tip Examine your network setup for guidance on how to best configure these settings.
Prefix Length	Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP.
Default Gateway	Specify the IP address of the default gateway for the adapter.
Primary DNS Server	Specify the DNS server address.
Secondary DNS server	Specify the DNS server address.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Apply**.

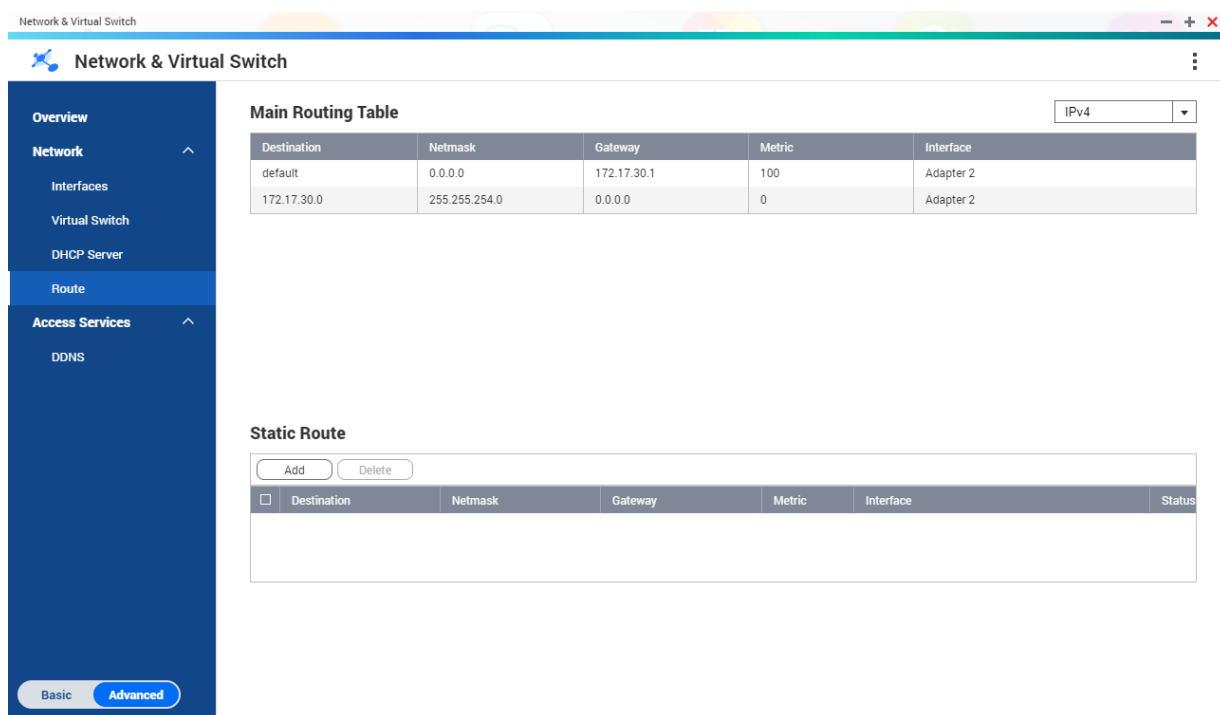
11. Configure the RADVD server settings.

Setting	Description
Prefix	Specify the routing prefix for the adapter.  Tip Examine your network setup for guidance on how to best configure these settings.
Prefix Length	Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Primary DNS Server	Specify the DNS server address.
Secondary DNS server	Specify the DNS server address.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

12. Click **Apply**.

Route

This screen controls the creation of static routes. Under normal circumstances, QTS automatically obtains routing information after it has been configured for Internet access. Static routes are only required in special circumstances, such as having multiple IP subnets located on your network.



Creating a Static Route

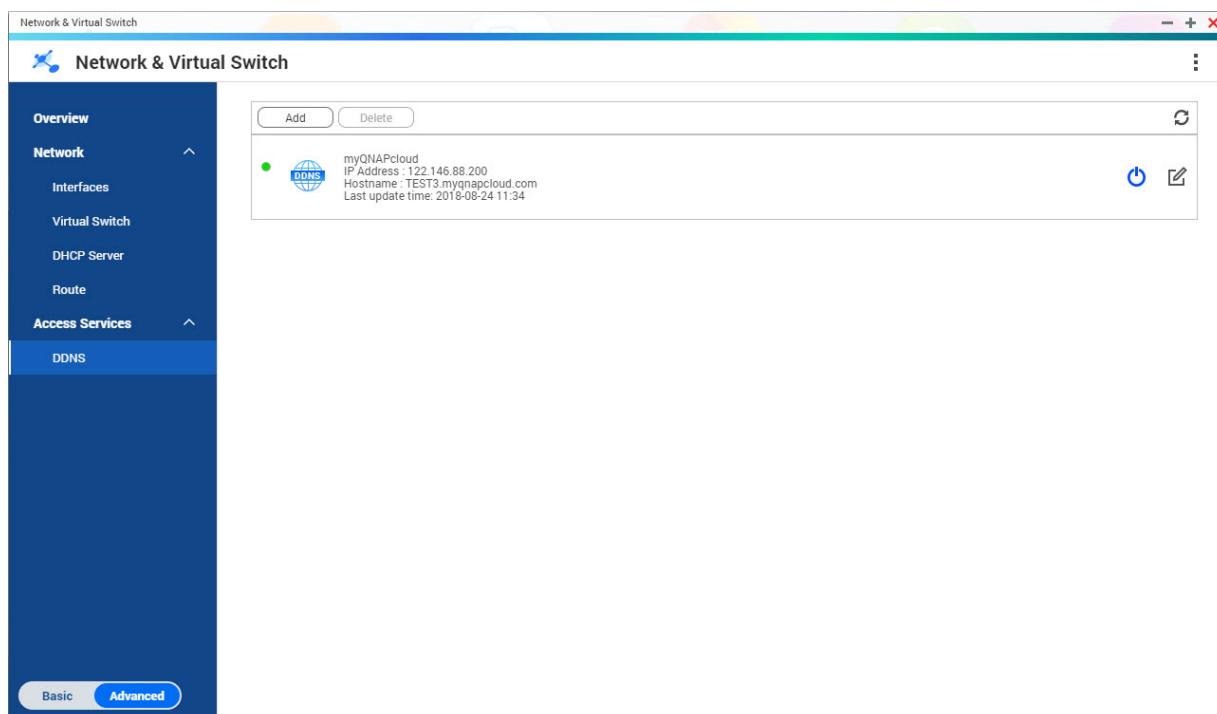
1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Route** .
3. Click **Add**.
The **Static Route (IPv4)** window opens.
4. Configure the IP address settings.

Setting	Description
Destination	Specify a static IP address where connections are routed to.
Netmask	Specify the IP address of the destination's netmask.
Gateway	Specify the IP address of the destination's gateway.
Metric	Specify the number of nodes that the route will pass through.  Note Metrics are cost values used by routers to determine the best path to a destination network.
Interface	Select the interface that connections should be routed through.

5. Click **Apply**.

DDNS

This screen controls the management of Dynamic Domain Name System (DDNS) services. DDNS allows access to the NAS from the internet using a domain name rather than an IP address.



Adding a DDNS Service

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DDNS** .
3. Click **Add**.
The **DDNS (Add)** window opens.
4. Configure the DDNS settings.

Setting	Description
Select DDNS server	Select the DDNS service provider.
Username	Specify the username for the DDNS service.
Password	Specify the password for the DDNS service.
Hostname	Specify the hostname or domain name for the DDNS service.
Check the External IP Address	Specify how often to update the DDNS record.

5. Click **Apply**.

7. Network & File Services

Network Access

Service Binding

NAS services run on all available network interfaces by default. Service binding enables you to bind services to specific network interfaces to increase security. You can bind services to one or more specific wired or wireless network interfaces.



Important

Configuring service binding does not affect users currently connected to the NAS. When users reconnect they will only be able to access the configured services using the specified network interfaces.

Configuring Service Binding

1. Go to **Control Panel > Network & File Services > Network Access > Service Binding**.
2. Select **Enable Service Binding**.
A list of available services and interfaces is displayed.
3. Bind services to interfaces.



Important

- By default, QTS services are available on all network interfaces.
- Services must be bound to at least one interface.



Tip

Click **Use Default Value** to bind all services.

- a. Identify a service.
 - b. Deselect interfaces not bound to the service.
4. Click **Apply**.

Proxy

A proxy server acts as an intermediary between the NAS and the internet. When enabled, QTS will route internet requests through the specified proxy server.

Configuring the Proxy Server Settings

1. Go to **Control Panel > Network & File Services > Network Access > Proxy**.
2. Select **Use a proxy server**.
3. Specify the proxy server URL or IP address.
4. Specify a port number.
5. Optional: Configure proxy authentication.

- a. Select **Authentication**.
- b. Specify a username.
- c. Specify a password.

6. Click **Apply**.

Win/Mac/NFS

Microsoft Networking

Microsoft Networking refers to Samba, a network protocol that allows data to be accessed over a computer network and provides file and print services to Windows clients.

Configuring Microsoft Networking

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > Microsoft Networking**.
2. Select **Enable file service for Microsoft networking**.
3. Configure Microsoft networking settings.

Setting	User Action
Server description (Optional)	Specify a description that contains a maximum of 256 characters. The description must enable users to easily identify the NAS on a Microsoft network.
Workgroup	Specify a workgroup name that contains 1 to 15 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: ~ ! @ # \$ ^ & () - _ { } . ' .

4. Select an authentication method.

Option	Description
Standalone server	QTS uses the local user account information for authentication.
AD domain member	QTS uses Microsoft Active Directory (AD) for authentication.
LDAP domain authentication	QTS uses an LDAP directory for authentication.

5. Configure the advanced settings.
 - a. Click **Advanced Options**.
The **Advanced Options** window opens.
 - b. Configure the advanced settings.

Option	User Action
Enable WINS server	Select this option to run a WINS server on the NAS.

Option	User Action
Use the specified WINS server	Select this option to specify a WINS server IP address that QTS will use for name resolution. Do not select this option if you are unsure about the settings.
Local master browser	Select this option to use the NAS as a local master browser. A local master browser is responsible for maintaining the list of devices in a specific workgroup on a Microsoft network. When deselected, another device on the network maintains the device list.  Important To use the NAS as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".
Allow only NTLMSSP authentication	Select this option to authenticate clients using only NT LAN Manager Security Support Provider. When this option is deselected, QTS uses NT LAN Manager (NTLM).
Name resolve priority	Select a name service to use for name resolution. The default service is DNS only . If a WINS server is specified, Try WINS then DNS is selected by default.
Login Style	Select this option to change how usernames are structured when accessing FTP, AFP, or File Station services. After selecting this option, users can access NAS services using Domain\Username, instead of Domain+Username.
Automatically register in DNS	Select this option to register the NAS on the DNS server. If the NAS IP address changes, the NAS automatically updates the IP address on the DNS server. This option is only available if AD authentication is enabled.
Enable trusted domains	Select this option to join users from trusted AD domains. This option is only available if AD authentication is enabled.
Enable Asynchronous I/O	Select this option to improve the Samba performance using asynchronous I/O. Asynchronous I/O refers to the I/O behavior on the CIFS protocol layer. This is different from the synchronous I/O feature found in the shared folder settings, which only applies to specific shared folders on the file system level.  Tip To prevent power interruption, use a UPS when asynchronous I/O is enabled.
Enable WS-Discovery	Select this option to enable Web Services Dynamic Discovery (WS-Discovery). WS-Discovery makes the NAS visible in File Explorer on Windows 10 computers.
Highest SMB version	Select the highest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.  Note Selecting SMB3 will also include SMB3.1 and SMB3.1.1.

Option	User Action
Lowest SMB version	Select the lowest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.  Note Selecting SMB3 will also include SMB3.1 and SMB3.1.1.
Allow Symbolic links within a shared folder	Select this option to allow symbolic links within shared folders.
Allow Symbolic links between different shared folders	Select this option to allow symbolic links between shared folders.  Note This setting requires Allow Symbolic links within a shared folder to be selected first.
Restrict anonymous users from accessing SMB shared folders	Select this option to require users to log in before accessing SMB shared folders.  Note This setting will be locked to Enabled (strict) if ABSE is enabled on any shared folder.

- c. Click **Apply**.
The **Advanced Options** window closes.

6. Click **Apply**.

Apple Networking

The Apple Filing Protocol (AFP) is a file service protocol that allows data to be accessed from a macOS device.

Configuring Apple Networking

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > Apple Networking**.
2. Select **Enable AFP (Apple Filing Protocol)**.
3. Optional: Select **DHX2 authentication support**.
4. Click **Apply**.

NFS Service

Network File System (NFS) is a file system protocol that allows data to be accessed over a computer network. Enabling the NFS service allows Linux and FreeBSD users to connect to the NAS.

Enabling the NFS Service

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > NFS Service**.
2. Enable NFS Service.
 - a. Optional: Click **Enable NFS v2/v3 Service**.

- b. Optional: Click **Enable NFS v4 Service**.
- 3. Click **Apply**.

Telnet/SSH

Telnet is a network protocol used to provide a command line interface for communicating with the NAS.

Secure Shell (SSH) is a network protocol used for securely accessing network services over an unsecured network. Enabling SSH allows users to connect to the NAS using an SSH-encrypted connection or a SSH client such as PuTTY.

SSH File Transfer Protocol (SFTP) is a secure network protocol that works with SSH connections to transfer files and navigate through the QTS filesystem. SFTP can be enabled after allowing SSH connections on the NAS.

Configuring Telnet Connections



Important

Only administrator accounts can access the NAS through Telnet.

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.
2. Select **Allow Telnet connection**.
3. Specify a port number.
Port numbers range from 1 to 65535.



Tip

The default Telnet port is 13131.

4. Click **Apply**.

Configuring SSH Connections



Important

Only administrator accounts can access the NAS through SSH.

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.
2. Select **Allow SSH connection**.
3. Specify a port number.
Port numbers range from 1 to 65535.



Tip

The default SSH port is 22.

4. Optional: Select **Enable SFTP**.
5. Click **Apply**.

Editing SSH Access Permissions

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.

- Click **Edit Access Permission**.
The **Edit Access Permission** window opens.

- Select user accounts to give access permissions.



Important

Only administrator accounts can log in using an SSH connection.

- Click **Apply**.

SNMP

The Simple Network Management Protocol (SNMP) is used to collect and organize information about managed devices on a network. Enabling the QTS SNMP service allows for the immediate reporting of NAS events, such as warnings or errors, to a Network Management Station (NMS).

Configuring SNMP Settings

- Go to **Control Panel > Network & File Services > SNMP**.
- Select **Enable SNMP Service**.
- Configure the SNMP settings.

Setting	User Action
Port number	Specify the port that the Network Management Station (NMS) will use to connect to QTS.
SNMP Trap Level	Select the type of alert messages that the NAS will send to the NMS. • Information: QTS sends information regarding ongoing or scheduled NAS operations. • Warning: QTS sends alerts when NAS resources are critically low or the hardware behaves abnormally. • Error: QTS sends alerts failing to enable or update NAS features or applications.
Trap Address	Specify the IP addresses of the NMS. You can specify a maximum of 3 trap addresses.

- Select the SNMP version that the NMS uses.

Option	User Action
SNMP V1/V2	Specify an SNMP community name that contains 1 to 64 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and the NAS. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.

Option	User Action
SNMP V3	Specify the username, authentication protocol and password, and privacy protocol and password. a. Specify a username.  Note The username should contain 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ b. Optional: Select Use Authentication. 1. Specify the authentication protocol.  Tip You can select either HMAC-MD5 or HMAC-SHA. If you are unsure about this setting, QNAP recommends selecting HMAC-SHA. 2. Specify an authentication password that contains 8 to 64 ASCII characters. c. Optional: Select Use Privacy. 1. Specify a privacy password that contains 8 to 64 ASCII characters.

5. Click **Apply**.

SNMP Management Information Base (MIB)

The Management Information Base (MIB) is a type of database in ASCII text format that is used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the NAS status or understand the messages that the NAS sends within the network. You can download the MIB and then view the contents using any word processor or text editor.



Important

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 you can read or set using SNMP. You must assign the correct OID to retrieve the NAS information. The default OID for QNAP NAS devices is 1.3.6.1.4.1.24861.2.

Downloading the SNMP MIB

1. Go to **Control Panel > Network & File Services > SNMP**.

2. Under **SNMP MIB**, click **Download**.
QTS downloads the NAS.mib file on your computer.

Service Discovery

UPnP Discovery Service

Universal Plug and Play (UPnP) is a networking technology that enables the discovery of networked devices connected to the same network. After enabling this service, devices supporting UPnP can discover the NAS.

Enabling the UPnP Discovery Service

1. Go to **Control Panel > Network & File Services > Service Discovery > UPnP Discovery Service**.
2. Select **Enable UPnP Discovery Service**.
3. Click **Apply**.

Bonjour

Bonjour is a networking technology developed by Apple that enable devices on the same local area network to discover and communicate with each other.

Enabling Bonjour

1. Go to **Control Panel > Network & File Services > Service Discovery > Bonjour**.
2. Select **Enable Bonjour Service**.
3. Select the services to be advertised by Bonjour.



Important

You must enable the services in QTS before advertising them with Bonjour.

4. Click **Apply**.

Network Recycle Bin

The Network Recycle Bin contains files deleted from the NAS through File Station, QuFTP, or by clients connected using Microsoft networking.

Configuring the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin**.
2. Select **Enable Network Recycle Bin**.
3. Optional: Configure the Network Recycle Bin settings.

Setting	Description
File retention time	Specify the number of days files are retained. The Daily check time controls when recycled files are checked against the retention time.  Tip This field supports a maximum of 9999 days. The default is 180 days.
Exclude these file extensions	Specify which file extensions are excluded from the Network Recycle Bin.  Important File types are case insensitive and must be separated by a comma.

4. Click **Apply**.

Deleting All Files in the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin**.
2. Click **Empty All Network Recycle Bin**.
A warning message appears.
3. Click **OK**.
QTS deletes all files from the Network Recycle Bin.

Restricting Access to the Network Recycle Bin

1. Go to **Control Panel > Privilege > Shared Folders**.
2. Identify a shared folder.
3. Under **Actions**, click .
The **Edit Properties** window appears.
4. Select **Enable Network Recycle Bin**.
5. Select **Restrict the access to Recycle Bin to administrators only for now**.
6. Click **OK**.

8. File Station

Overview

About File Station

File Station is a QTS file management application that allows you to access files on the NAS. You can quickly locate files and folders, manage access permissions, play media files, and share data with other users.

System Requirements

Category	Detail
Web browser	• Microsoft Internet Explorer 9 or later • Microsoft Edge • Mozilla Firefox 3.6 or later • Apple Safari 5 or later • Google Chrome
Java program	Java Runtime Environment (JRE) 7 or later
Flash player	Adobe Flash Player 9 or later is required for viewing media files.

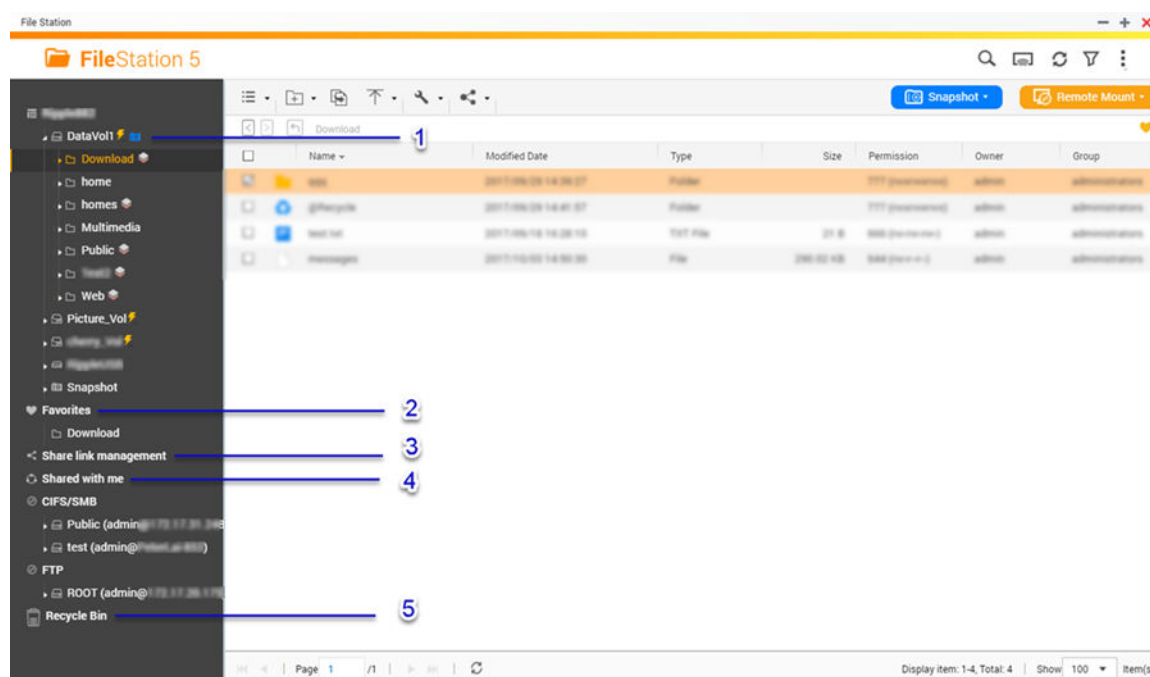
Supported File Formats

Category	File Extension
Image	• BMP • JPG • JPE • PNG • TGA • GIF
Music	• MP3 • FLAC • OGG • WAV • AIF • AIFF

Category	File Extension
Video	• AVI • MP4

Parts of the User Interface

Left Panel



Label	UI Element	Description
1	Volume	Displays all the folders in the volume, including shared folders. The default shared folders vary depending on the NAS model.
2	Favorites	Displays bookmarked folders.
3	Share link management	Displays links to NAS files shared by the current user account.  Note Administrators see links shared by all NAS users.
4	Share with me	Displays files and folders shared with the current user account.
5	Recycle Bin	Displays deleted files and folders.

Depending on your setup, the following folders may also appear on the list.

Folder	Description
Snapshot	Displays the saved snapshots from enabled volumes.

Folder	Description
Local folders	Displays the local folders on a Windows computer.  Important To view local folders from File Station, you must first install Java Runtime Environment.
Qsync	Displays files, folders, and team folders from Qsync.

Volume Icons

Depending on your NAS model and environment, the following icons may appear beside each available volume.

Icon	Description
	On Demand Tiering The icon appears when auto tiering is enabled on the volume.
	Snapshots The icon appears when snapshots are available for the volume. For details, go to the Snapshots section of the QTS User Guide.
	Cache Acceleration The icon appears when acceleration is enabled on the volume.
	Volume Encryption This icon appears when the volume is encrypted.

Left Panel Tasks

You can perform the following tasks for a volume on the left panel.



Tip

To see the task options, hover the mouse point over a volume and then click .

Task	Description
Create a shared folder	Click to create a shared folder. For details, see Creating a Shared Folder .
Open Snapshot Manager	Click to open Snapshot Manager. For details, see the Snapshots section of the QTS User Guide.
Lock/Unlock the volume	Click to lock or unlock an encrypted volume in Storage & Snapshots.

Menu Bar



Label	Item	Description
1	Search	Search files and folders by their name or type.  Tip You may select Advanced Search to specify more criteria.
2	Network Media Player	Stream videos, photos, and music to compatible devices on your network.
3	Refresh	Refresh the current page.
4	Smart Filter	Filter files and folders based on the specified criteria.
5	More Settings	Configure File Station settings, open the Help guide, or view application information.
6	Browsing Mode	Select a browsing mode.
7	Create folder	Create a folder, shared folder, snapshot shared folder, or share a space with another NAS user.
8	Copy	Copy the selected files and folders.  Note This button only appears when a file or folder is selected.
9	Upload	Upload files or folders to the selected shared folder.
10	More Action	Perform different tasks. The list of available actions changes after selecting a file or folder.
11	Share	Share the selected files and folders.  Note This button only appears when a file or folder is selected.
12	Snapshot	Open the Snapshot Manager or view the Snapshot Manager quick tutorial.
13	Remote Mount	Manage files across local, external, remote, and cloud storage resources on a single interface.
14	Add to Favorites	Add the current folder to your list of favorite folders.

Settings

Modifying the General Settings

1. Click  on the top-right corner.
2. Select **Settings**.
The **Options** window appears.
3. Select **General**.
4. Modify the following general settings as needed.

Option	Description
Show files and folders of my PC	File Station displays the local files and folders on the computer. This feature only supports Windows computers and requires the installation of Java Runtime Environment.
Show hidden files on NAS	File Station displays files and folders with the hidden attribute.
Allow all users to create shared links	All users can share data from the NAS using shared links.
Support multimedia playback and thumbnail display	File Station allows on-the-fly transcoding and displays thumbnail previews of multimedia files.
Always display the 360° panoramic view button on the viewer	File Station permanently displays the 360° panoramic view button and allows users to manually switch between the panorama and general modes.
Show Network Recycle Bin(s)	File Station displays the @Recycle folder in all user folders.
Only allow the admin and administrators group to use "Share to NAS user"	File Station prevents non-administrators from sharing files with other NAS users.
Only allow the admin and administrators group to permanently delete files	File Station prevents non-administrators from permanently deleting files.
Only allow the admin and administrators group to use on-the-fly transcoding	File Station prevents non-administrators from using on-the-fly transcoding.

5. Click **Close**.

Modifying the Remote Mount Settings

1. Click  on the top-right corner.
2. Select **Settings**.
The **Options** window appears.
3. Select **Remote Mount**.
4. Select one of the following remote access permissions.
 - admin only
 - administrators group only
 - specific users

5. Click **Apply**.

Modifying the File Transfer Settings

1. Click  on the top-right corner.
2. Select **Settings**.
The **Options** window appears.
3. Select **File Transfer**.
4. Select one of the following policies for handling duplicate files.
 - **Always ask me**
 - **Rename duplicate files**
 - **Skip duplicate files**
 - **Overwrite duplicate files**
5. Optional: Select **Always merge all file transfer processes into one task**.
6. Click **Apply**.

File Operations

File Station enables you to perform the following tasks.

Operation	Task
Store	• Uploading a File
Access	• Downloading a File • Opening a File • Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension • Opening a Text File Using Text Editor • Viewing a File in Google Docs • Viewing a File in Microsoft Office Online • Viewing File Properties • Modifying File Permissions

Operation	Task
Organize	• Sorting Files • Copying a File • Moving a File • Renaming a File • Deleting a File • Restoring a Deleted File • Mounting an ISO File • Unmounting an ISO File • Compressing a File • Extracting Compressed Files or Folders.
Share	• Sharing a File or Folder by Email • Sharing a File or Folder on a Social Network • Sharing a File or Folder Using Share Links • Sharing a File or Folder with a NAS User
Play	• Playing a Video File • Opening a 360-degree Image or Video File • Streaming to the Network Media Player
Transcode	• Adding a File to the Transcode Folder • Canceling or Deleting Transcoding • Viewing Transcode Information

Uploading a File

1. Open File Station.
2. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Click  and then select File. The File Upload window opens. b. Select the file and then click Open.
Use drag and drop	a. Locate the file on your computer. b. Drag and drop the file to the File Station window.

A confirmation message appears.

3. Select one of the following policies for handling duplicate files.

Option	Description
Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.



Tip

You can set the selected option as the default policy. File Station will not ask again after remembering the setting. You can still change the policy in **File Station > More Settings > Settings > File Transfer**.

4. Click **OK**.
File Station uploads the file.

Downloading a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Download. d. Click OK.
Use the context menu	Right-click the file and then click Download .

Depending on your browser, a confirmation message appears before the file is downloaded to your computer.

Opening a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click .

	c. Select Open.
Use the context menu	Right-click and then select Open .

File Station opens the selected file.

Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension

This task requires that you use the Google Chrome browser and install the Office Editing for Docs, Sheets & Slides extension.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Open with Chrome Extension.
Use the context menu	Right-click the file and then select Open with Chrome Extension .

File Station opens an editable file on Google Docs, Sheets, or Slides.

Opening a Text File Using Text Editor

This task requires that you install Text Editor from the App Center.

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Open with Text Editor.
Use the context menu	a. Right-click the file. b. Select Open with Text Editor.

File Station opens the selected text file using Text Editor.

Viewing a File in Google Docs

This task requires that you use the Google Chrome browser and enable myQNAPcloud Link.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select View in Google docs.
Use the context menu	Right-click and then select View in Google docs .

File Station opens a preview of the file in Google Drive.

Viewing a File in Microsoft Office Online

This task requires that you enable myQNAPcloud Link.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select View in Office Online.
Use the context menu	Right-click and then select View in Office Online .

File Station opens a preview of the file in Microsoft Office Online.

Viewing File Properties

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file.

	b. Click  . c. Select Properties .
Use the context menu	a. Right-click the file. b. Select Properties .

The **Properties** window opens and displays the following information.

Field	Description
Type	Displays the file type.
Size	Displays the file size.
File Path	Displays the folder location.
Modified Date	Displays the date that the file was last modified.
Owner	Displays name of the NAS user who uploaded the file.
Group	Displays the name of the NAS group that can access the file.
Storage Pool	Displays the name of the storage pool on which the volume is located.
Volume	Displays the name of the volume on which the file is stored.

Modifying File Permissions

This task requires that you enable advanced folder permissions in **Control Panel > Privilege > Shared Folders > Advanced Permissions**.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click  . c. Select Properties .
Use the context menu	a. Right-click the file. b. Select Properties .

The **Properties** window opens and displays the following information.

4. Click .
5. Enable or disable the following permissions for the owner, group, and other users on the list.

Permission	Description
Read Only	Allows a user to view the file.
Read/Write	Allows a user to view the file and make changes to the file.

Deny	Denies any access to the file
------	-------------------------------

**Tip**

You can click **+** to add users to the list and click **-** to remove users from the list.

6. Optional: Specify the access right for guest users.
7. Optional: Specify the owner of this file.
8. Click **Apply**.

Sorting Files

1. Open File Station.
2. Locate the folder.
3. Click .
Click .
4. Select **List**.
File Station displays files in a list view.
5. Click a column title.
File Station sorts files in an ascending or descending order based on the selected column.

Copying a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . Click . c. Select Copy to/Move to and then select Copy to. d. Select the destination folder. e. Click OK.
	a. Select the file. b. Click Copy. c. Go to the destination folder. d. Click Paste.
Use the context menu	a. Right-click the file. b. Select Copy. c. Go to the destination folder.

	d. Right-click inside the folder and then select Paste.
Use keyboard shortcuts	a. Select the file. b. Press CTRL + C or Command-C. c. Go to the destination folder. d. Press CTRL + V or Command-V.
Use drag and drop	a. Select the file. b. Drag and drop to the destination folder. Step result: A context menu appears. c. Select one of the following actions. • Copy and skip • Copy and overwrite • Copy and rename automatically

File Station creates a copy of the selected file.

Moving a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b.  Click . c. Select Copy to/Move to and then select Move to. d. Select the destination folder. e. Click OK.
	a. Select the file. b.  Click . c. Select Cut. d. Select the destination folder. e.  Click . f. Select Paste.
Use the context menu	a. Right-click the file and then select Copy to/Move to and Move to.

	b. Select the destination folder. c. Click OK.
	a. Right-click the file and then select Cut. b. Select the destination folder. c. Right-click inside the folder and then select Paste.
Use keyboard shortcuts	a. Select the file. b. Press CTRL + X or Command-X. c. Go to the destination folder. d. Press CTRL + V or Command-V.
Use drag and drop	a. Select the file. b. Drag and drop to the destination folder. c. Step result: A context menu appears. d. Select one of the following actions. • Move and skip • Move and overwrite • Move (and rename if a file exists with the same name)

File Station moves the selected file to the specified folder.

Renaming a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Rename.
Use the context menu	a. Right-click the file. b. Select Rename.
Use a keyboard shortcut.	Press F2 .

4. Specify the file name and then click **OK**.
File Station renames the file.

Deleting a File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Delete.
Use the context menu	a. Right-click the file. b. Select Delete.
Use the keyboard	Press Delete .

A confirmation message appears.

4. Specify how to delete the file.
 - Move to Network Recycle Bin
 - Delete permanently
5. Click **OK**.
File Station either moves the selected file to the Recycle Bin or deletes it permanently.

Restoring a Deleted File

1. Open File Station.
2. Go to **Recycle Bin**.
3. Locate the file.
4. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Recover.
Use the context menu	a. Right-click the file. b. Select Recover.

A confirmation message appears.

5. Click **Yes**.

File Station restores the selected file.

Mounting an ISO File

1. Open File Station.
2. Upload an ISO file.
For details, see [Uploading a File](#).
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Mount ISO.
Use the context menu	a. Right-click the file. b. Select Mount ISO.

The **Mount ISO** window appears.

4. Specify the shared folder name.
5. Click **OK**.
File Station mounts the ISO file as a shared folder.

Unmounting an ISO File

1. Open File Station.
2. On the left panel, locate the mounted ISO file.
3. Right-click the file and then select **Unmount**.
A confirmation message appears.
4. Click **Yes**.
File Station unmounts the ISO file and displays a confirmation message.
5. Click **OK**.

Compressing a File

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file or folder. b. Click .

	c. Select Compress(Zip).
Use the context menu	a. Right-click the file or folder. b. Select Compress(Zip).

4. Configure the file compression settings.

Option	Task
Archive name	Specify a name for the compressed file.
Compression level	Select the type of compression method. • Normal - Standard compression • Maximum compression - Prioritizes compression quality • Fast compression - Prioritizes compression speed
Archive format	Select the format of file compression. • zip • 7z
Update mode	Specify how the files should be updated. • Add and replace files - Add and replace the specified files. • Update and add files - Update old files and add new files. • Update existing files - Update older versions of existing files. • Synchronize files - Update old files, add new files, and remove files that are no longer in the folder.

5. Optional: Specify a password to encrypt the file.

6. Click **OK**.

File Station compresses the selected file and creates a archive file.

Extracting Compressed Files or Folders.

1. Open File Station.
2. Locate the compressed archive file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click  . c. Select Extract.
Use the context menu	a. Right-click the file. b. Select Extract.

4. Select one of the following extraction options.

Option	Description
Extract files	Select specific files to extract.
Extract here	Extract all files in the current folder.
Extract to /<new folder>/	Extract all files in a new folder. The new folder uses the file name of the compressed file.

File Station extracts the compressed files to the specified folder.

Sharing a File or Folder by Email

Before starting this task, you must configure the QTS email settings in **QTS Desktop** >  > **E-mail Account**.

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file or folder b. Click Share. c. Select Via Email.
Use the context menu	a. Right-click the file or folder. b. Select Share. c. Select Via Email.

The **Share** window appears.

4. Configure the following settings.

Field	Description
Send from	Select the email delivery method. • Use NAS to mail the link(s). • Use local computer to mail the link(s).
Sender	Select an email account.
To	Specify the email address of the recipient.  Tip You can select a recipient from your contact list if Qcontactz is installed on the NAS.
Subject	Specify the email subject.
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	Task
Link Name	Enter a name for the link or use the current name of the file or folder.
Domain name/IP	Select the domain name or IP address.
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	Allow users to transcode videos on the fly.  Note • This setting only appears when you share video files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder.  Note This setting only appears when you share a folder.
Expire in	Specify the expiration date.  Note You cannot access the shared file or folder after the expiration date.
Password	Require a password to access the link.  Tip You can choose to include the password in the email.

- Click **Share Now**.
File Station sends an email to the recipient.

Sharing a File or Folder on a Social Network

- Open File Station.
- Locate the file or folder.
- Perform one of the following methods.

Method	Steps
Use the menu bar	- Select the file or folder. - Click Share. - Select To Social Network.
Use the context menu	- Right-click the file or folder. - Select Share and then select To Social Network.

The **Share** window appears.

- Configure the following settings.

Field	Description
-------	-------------

Social Network	Select the social network website.
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	Task
Link Name	Type a name for the link or use the current file or folder name.
Domain name/IP	Select the domain name or IP address.
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	Allow users to transcode videos on the fly.  Note - This setting only appears when you share video files. - To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder  Note This setting only appears when you share a folder.
Expire in	Specify the expiration date.  Note You cannot access the shared file or folder after the expiration date.
Password	Require a password to access the link.

6. Click **Share Now**.
File Station connects to the specified social network website.

Sharing a File or Folder Using Share Links

- Open File Station.
- Locate the file or folder.
- Perform one of the following methods.

Method	Steps
Use the menu bar	- Select the file or folder. - Click Share. - Select Create share link only.
Use the context menu	- Right-click the file or folder. - Select Share and then select Create share link only.

The **Share** window appears.

- Configure the following settings.

Field	Task
Link Name	Type a name for the link or use the current file or folder name.
Domain name/IP	Select the domain name or IP address.
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	Allow users to transcode videos on the fly.  Note - This setting only appears when you share video files. - To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder  Note This setting only appears when you share a folder.
Expire in	Specify the expiration date.  Note This setting only appears when you share a folder.
Password	Require a password to access the link.

- Click **Create Now**.
File Station generates a link.

Sharing a File or Folder with a NAS User

- Open File Station.
- Locate the file or folder.
- Perform one of the following methods.

Method	Steps
Use the menu bar	- Select the file or folder. - Click Share. - Select To NAS user.
Use the context menu	- Right-click the file or folder. - Select Share and then select To NAS user.

The **Share** window appears.

- Select the user to share the file or folder with.

Option	Description
Existing user	Select a user from the list. Optional: Select Send a notification email to the user and then specify the email subject and message. Only users who have provided email information will receive notifications.

	 Note You can specify the email information of each user in Control Panel > Privilege > Users .
New user	Create a new user account.

5. Optional: Click **More settings** and configure additional settings.

Field	Task
Link Name	Type a name for the link or use the current file or folder name.
Domain name/IP	Select the domain name or IP address.
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	Allow users to transcode videos on the fly.  Note • This setting only appears when you share video files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder  Note This setting only appears when you share a folder.
Expire in	Specify the expiration date.  Note You cannot access the shared file or folder after the expiration date.
Password	Require a password to access the link.

6. Click **Share Now**.
 File Station shares the file with the specified user.

Playing an Audio File

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b.  Click . c. Select Play.
Use the context menu	a. Right-click the file. b. Select Play.

File Station plays the selected audio file using Media Viewer.

Playing a Video File

You must install Video Station from App Center to play certain video formats.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Play. d. Select a resolution.
Use the context menu	a. Right-click the file. b. Select Play. c. Select a resolution.

File Station plays the selected file using Media Viewer.

Opening Image Files Using Image2PDF

You must to install Image2PDF from the App Center before starting this task.

1. Opening File Station
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Open with Image2PDF.
Use the context menu	Right-click and then select Open with Image2PDF .

File Station opens the selected image file with the Image2PDF wizard.

Follow the wizard's on-screen instructions to convert the image file into a PDF file.

Opening a 360-degree Image or Video File

1. Open File Station.
2. Locate the folder.

3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Play.
Use the context menu	a. Right-click the file. b. Select Play.

4. Optional: Select the resolution.

File Station opens the selected file using the Media Viewer. You can click **360 Panorama Mode** () on Media Viewer to view the photo or video in Panorama Mode.

Streaming to the Network Media Player

This task requires that you install Media Streaming add-on from the App Center.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click Network Media Player () on the menu bar. c. Select the media player. The Media Viewer window appears. d. Select Play the selected item on this player. e. Click OK.
	a. Select the file. b. Click . c. Select Streaming to. d. Under Network Media Player, select a media player.
Use the context menu	a. Right-click the file. b. Select Streaming to. c. Under Network Media Player, select a media player.

File Station plays the selected file using the specified network media player.

Adding a File to the Transcode Folder



Important

Video files cannot be converted to a resolution higher than the original one. If a higher resolution is selected, File Station automatically uses the original resolution when transcoding the file.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b.  Click . c. Select Add to Transcode.
Use the context menu	a. Right-click the file. b. Select Add to Transcode.

The **Add to Transcode** window opens.

4. Select the transcoding video resolution.
 - 240p
 - 360p
 - 480p SD
 - 720p HD
 - 1080 FULL HD
5. Click **OK**.
File Station adds the selected file to the Transcode folder.

Canceling or Deleting Transcoding

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b.  Click . c. Select Cancel/Delete Transcoding.

Use the context menu	a. Right-click the file. b. Select Cancel/Delete Transcoding.
----------------------	---

A confirmation message appears.

4. Click **OK**.

File Station removes the selected file from the Transcode folder and cancels the transcoding process.

Viewing Transcode Information

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the file. b. Click . c. Select Transcode Information.
Use the context menu	a. Right-click the file. b. Select Transcode Information.

The **On-the-fly Transcoding Task** screen appears.

Folder Operations

File Station enables you to perform the following tasks.

Operation	Task
Store	• Uploading a Folder • Uploading a Folder Using Drag and Drop
Access	• Viewing and Modifying Folder Properties • Viewing Storage Information • Modifying Folder Permissions • Viewing Qsync Folders • Managing Share Links • Viewing Files and Folders Shared with Me

Operation	Task
Organize	• Creating a Folder • Copying a Folder • Creating a Desktop Shortcut • Adding a Folder to Favorites • Removing a Folder from Favorites • Compressing a Folder
Share	• Creating a Shared Folder • Creating a Snapshot Shared Folder • Sharing Space with a New User
Transcoding	• Adding a Folder to the Transcode Folder • Canceling or Deleting Transcoding

Uploading a Folder



Note

This feature is only available on Google Chrome browsers.

1. Open File Station.
2. Open the destination folder.
3. Click  and then select **Folder**.
The **Browse for Folder** window opens.
4. Select the folder to upload.
A confirmation message appears.
5. Select one of the following policies for handling duplicate files.

Option	Description
Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.



Tip

You can set the selected option as the default policy. File Station will not ask again after remembering the setting. You can change the policy later in **File Station > More Settings > Settings > File Transfer**.

6. Click **OK**.
File Station uploads the selected folder.

Uploading a Folder Using Drag and Drop



Note

This feature is only available on Google Chrome browsers.

1. Open File Station.
2. Drag and drop the local folder to File Station.
3. Select one of the following policies for handling duplicate files.

Option	Description
Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.

4. Click **OK**.
File Station uploads the selected folder.

Viewing and Modifying Folder Properties

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Properties.
Use the context menu	a. Position the mouse pointer inside the folder. b. Right-click the folder. c. Select Properties.
Use the left panel	a. Right-click the folder. b. Select Properties.

The **Properties** window opens and displays the following information.

Field	Description
Type	Displays the folder type.
Size	Click  to display the folder size and total file count.
File Path	Displays the folder location.

Field	Description
Modified Date	Displays the date that the folder was last modified.
Owner	Displays name of the NAS user who uploaded the folder.
Group	Displays the name of the NAS group that can access the folder.
Storage Pool	Displays the name of the storage pool on which the volume is located.
Volume	Displays the name of the volume on which the folder is stored.
Media Folder	Select one or more of the following options to allow QTS to automatically scan and create thumbnail images of media files in the folder. • music • video • photo
Auto Transcoding Folder	Select one of the following resolutions to automatically convert video files in the folder to the MP4 format and use the specified resolution when playing video files. • 240p • 360p • 480p • 720p • 1080p

4. Modify advanced settings.

- a. Click **More settings>>**.
The **Edit Properties** window appears.
- b. Modify the following settings if needed.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Media Folder	Selecting this option allows media applications to scan this folder for media files.
Hide Network Drives	Selecting this option hides the folder in Windows networks. Users that know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	Selecting this option allows users to use the Previous Versions feature on Windows to restore the previous versions of this shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.

Option	Description
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.
Enable access-based share enumeration (ABSE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access. Guests must specify a username and password before viewing shared folders.
Enable access-based enumeration (ABE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access.
Set this folder as the Time Machine backup folder (macOS)	Selecting this option allows users to back up the data on the Mac to this shared folder via Time Machine.

c. Click **OK**.

5. Click **Apply**.

Viewing Storage Information

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Storage Info.
Use the context menu	a. Right-click the folder. b. Select Storage Info.

The **Storage Info** window opens and displays the following information.

Information	Description
Shared folder	Displays the names of shared folders.
Used size	Displays the total storage size currently in use.
Volume	Displays the volume name.
Capacity	Displays the total storage capacity of the shared folder.
Free size	Displays the total available storage space in the shared folder.
Volume status	Displays the volume status.

Modifying Folder Permissions

This task requires that you enable advanced folder permissions in **Control Panel > Privilege > Shared Folders > Advanced Permissions**.

1. Open File Station.

2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Properties.
Use the context menu	a. Right-click the folder. b. Select Properties.

The **Properties** window opens.

4. Click .
5. Enable or disable the following permissions for the owner, group, and other users on the list.

Permission	Description
Read Only	Allows a user to view the folder.
Read/Write	Allows a user to view and make changes to the folder.
Deny	Denies a user any access to the folder



Tip

You can click + to add users to the list and click - to remove users from the list.

6. Optional: Specify the access right for guest users.
7. Optional: Specify the owner of this folder.
8. Optional: Enable one or more of the following settings if needed.
 - Only the owner can delete the contents
 - Only admin can create files and folders
 - Apply changes to files and subfolders
 - Apply and replace all existing permissions
9. Click **Apply**.

Viewing Qsync Folders

1. Open File Station.
2. On the left panel, click **Qsync**.
File Station displays the list of team folders shared by other NAS users.

Managing Share Links

1. Open File Station.
2. On the left panel, click **Share link management**.
File Station displays the list of shared files and folders.
3. Select an item from the list and then perform one of the following tasks.

Task	Steps
Re-share	Click  and then select one of the following share methods. • Sharing a File or Folder by Email • Sharing a File or Folder on a Social Network • Sharing a File or Folder Using Share Links • Sharing a File or Folder with a NAS User
Stop sharing	Click  .
Copy the link to the clipboard	Click  .

File Station performs the specified task.

Viewing Files and Folders Shared with Me

1. Open File Station.
2. On the left panel, click **Shared with me**.

File Station lists the files and folders shared with the current account. You can copy, open, or download a selected file or folder.

Creating a Folder

1. Open File Station.
2. Locate the destination folder.
3. Perform one of the following tasks.

Task	Steps
Use the menu bar	a. Click . b. Select Folder. The Create folder window opens. c. Specify the folder name. d. Click OK.
Use the context menu	a. Right-click inside the folder and then select Create folder.

- b. Specify the folder name.
- c. Click **OK**.

File Station creates a new folder.

Copying a Folder

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b.  Click . c. Select Copy to/Move to and then select Copy to. d. Select the destination folder. e. Click OK.
Use the context menu	a. Right-click the folder. b. Select Copy. c. Go to the destination folder. d. Right-click inside the folder and then select Paste.

File Station creates a copy of the selected folder.

Creating a Desktop Shortcut

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b.  Click . c. Select Create Shortcut to Desktop.
Use the context menu	a. Right-click the folder. b. Select Create Shortcut to Desktop.
Drag and Drop	a. Select the folder.

- | | |
|--|---|
| | b. Drag and drop the folder to the desktop. |
|--|---|

File Station creates a desktop shortcut for the selected folder.


Tip

Hovering the mouse pointer over a desktop shortcut displays the path of the original folder.

Adding a Folder to Favorites

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Add to Favorites.
Use the context menu	a. Right-click the folder. b. Select Add to Favorites.
Use the Favorites button	a. Select the folder. b. Click .

File Station adds the selected folder to the Favorites folder.

Removing a Folder from Favorites

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Remove from Favorites.
Use the context menu	a. Right-click the folder. b. Select Remove from Favorites.
Use the Favorites button	a. Select the folder. b. Click .

File Station removes the selected folder from the Favorites folder.

Compressing a Folder

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Compress(Zip).
Use the context menu	a. Right-click the folder. b. Select Compress(Zip).

4. Configure the folder compression settings.

Option	Task
Archive name	Specify a name for the compressed file.
Compression level	Select the type of compression method. • Normal - Standard compression • Maximum compression - Prioritizes compression quality • Fast compression - Prioritizes compression speed
Archive format	Select the format of file compression. • zip • 7z
Update mode	Specify how the files should be updated. • Add and replace files - Add and replace the specified files. • Update and add files - Update old files and add new files. • Update existing files - Update older versions of existing files. • Synchronize files - Update old files, add new files, and remove files that are no longer in the folder.

5. Optional: Specify a password to encrypt the file.
6. Click **OK**.
File Station compresses the selected folder and creates an archive file.

Deleting a Folder

1. Open File Station.
2. Locate the folder.

3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click . c. Select Delete.
Use the context menu	a. Right-click the folder. b. Select Delete.
Use the keyboard	Press Delete .

A confirmation message appears.

4. Specify how to delete the folder.

- Move to Network Recycle Bin
- Delete permanently

5. Click **OK**.

File Station either moves the selected folder to the Recycle Bin or deletes it permanently.

Creating a Shared Folder

1. Open File Station.

2. On the menu bar, click .

3. Select **Shared Folder**.

The **Create A Shared Folder** window opens.

4. Configure the folder settings.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin with a space or "_sn_" • Contain consecutive spaces • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' .
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Disk Volume	Specify the volume on which the shared folder will be created.
Qtier auto Tiering	Select this option to enable auto-tiering for this folder.  Note To use this feature, you must enable Qtier on the storage pool.
Path	Specify a path manually or allow QTS to automatically select a path.

5. Optional: Configure user access permissions.
 - a. Under **Configure access privileges for users**, click **Edit**.
 - b. Specify access permissions for each user.
6. Optional: Enable folder encryption.
 - a. Under **Folder Encryption**, click **Edit**.
 - b. Select **Encryption**.
 - c. Configure the encryption settings.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " \$: = \
Verify Password	The password must match the previously specified password.
Save encryption key	When enabled, QTS automatically unlocks the shared folder after the NAS restarts. When disabled, the admin must perform the following steps: a. Restart the NAS. b. Go to Control Panel > Privilege > Shared Folders > Shared Folder. c. Click the unlock icon.  Warning The data will be inaccessible if the encryption password is lost.

7. Optional: Configure advanced settings.
 - a. Under **Advanced Settings**, click **Edit**.
 - b. Configure the following settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Media Folder	Selecting this option allows media applications to scan this folder for media files.
Hide Network Drives	Selecting this option hides the folder in Windows networks. Users that know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.

Option	Description
Enable Windows Previous Versions	Selecting this option allows users to use the Previous Versions feature on Windows to restore the previous versions of this shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.
Enable access-based share enumeration (ABSE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access. Guests must specify a username and password to view shared folders.
Enable access-based enumeration (ABE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access.
Set this folder as the Time Machine backup folder (macOS)	Selecting this option allows users to back up the data on the Mac to this shared folder via Time Machine.

- Click **OK**.
File Station creates a shared folder.

Creating a Snapshot Shared Folder

- Open File Station.
- On the menu bar, click .
- Select **Snapshot shared folder**.
The **Create a Snapshot Shared Folder** window opens.
- Configure the folder settings.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: - Begin with a space or "_sn_" - Contain consecutive spaces - Contain the following characters: " + = / \ : * ? < > ; [] % ` ' .
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Storage Pool	Specify the storage pool where this shared folder will be created.
Space Allocation	Select one of the following space allocation options: - Thick provisioning - Thin provisioning
Qtier Auto Tiering	Select this option to enable auto-tiering for this folder.  Note To use this feature, you must enable Qtier on the storage pool.
Allocate Folder Quota	Specify a data quota for the folder.

5. Optional: Configure user access permissions.
 - a. Under **Configure access privileges for users**, click **Edit**.
 - b. Specify access permissions for each user.
6. Optional: Configure advanced settings.
 - a. Under **Advanced Settings**, click **Edit**.
 - b. Configure the following settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Media Folder	Selecting this option allows media applications to scan this folder for media files.
Hide Network Drives	Selecting this option hides the folder in Windows networks. Users that know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	Selecting this option allows users to use the Previous Versions feature on Windows to restore the previous versions of this shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.
Enable access-based share enumeration (ABSE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access. Guests must specify a username and password to view shared folders.
Enable access-based enumeration (ABE)	When this option is enabled, users can only see the shared folders that they have permissions to mount and access.
Set this folder as the Time Machine backup folder (macOS)	Selecting this option allows users to back up the data on the Mac to this shared folder via Time Machine.

7. Click **Create**.
File Station creates a snapshot shared folder.

Sharing Space with a New User

1. Open File Station.
2. On the menu bar, click  .
3. Select **Share space with a user**.
The **Create a User** window opens.
4. Specify the following information:

Field	Description
Username	Specify a username that contains 1 to 32 characters from any of the following groups: - Letters: A to Z, a to z - Numbers: 0 to 9 - Special characters: ~ ! @ # \$ ^ & () - _ . { }
Password	Specify a password that contains 1 to 64 ASCII characters.
Quota	Specify the storage capacity available to the user.
Phone number (optional)	The information is for your reference and is not used by QTS.
Email (optional)	QTS sends a notification to this email address when the account password is about to expire.  Note - You must configure the related settings in SMTP Server and Change Password. Otherwise, QTS would not send notifications to the specified email address. SMTP Server: Go to Control Panel > System > Notification > E-mail. Change Password: Go to Control Panel > System > Security > Password Policy.
(Optional) Send a notification mail to the newly created user	When selected, QTS sends a message that contains the following information to the specified email address. - Username and password - URLs for connecting to the NAS

5. Click **Create**.

File Station creates a new user account and allocates the specified storage space.

Adding a Folder to the Transcode Folder



Important

Video files cannot be converted to a resolution higher than the original one. If a higher resolution is selected, File Station automatically uses the original resolution when transcoding the file.

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b. Click .

	c. Select Add to Transcode.
Use the context menu	a. Right-click the file. b. Select Add to Transcode.

The **Add to Transcode** window opens.

4. Select the transcoding video resolution.

- 240p
- 360p
- 480p SD
- 720p HD
- 1080 FULL HD

5. Click **OK**.

File Station adds the selected folder to the Transcode folder.

Canceling or Deleting Transcoding

1. Open File Station.
2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Use the menu bar	a. Select the folder. b.  Click  . c. Select Cancel/Delete Transcoding.
Use the context menu	a. Right-click the folder. b. Select Cancel/Delete Transcoding.

A confirmation message appears.

4. Click **OK**.

File Station removes the selected folder from the Transcode folder and cancels the transcoding process.

Remote Mount

About Remote Mount

The remote mount service allows you to manage files across local, external, remote, and cloud storage resources on a single interface. You can easily perform common file management tasks, such as copying and moving data between local and remote locations. The remote mount service supports many popular

cloud services and file sharing protocols, and can automatically detect available devices on the local network.

Remote Mount Limitations

Limitation	Detail
Maximum number of remote mounts per NAS	256
Maximum number of supported sharing links	1000
Supported browsers	• Microsoft Internet Explorer 9 or later • Microsoft Edge • Mozilla Firefox 3.6 or later • Apple Safari 5 or later • Google Chrome

Creating Remote Mount

Mounting a Cloud Drive

You must install the Connect to Cloud Drive app from App Center before starting this task.

1. Open File Station.
2. Click **Remote Mount** and then select **Create remote mount**.
The **Create remote mount** window opens.
3. Under **Cloud service**, select a cloud service.
4. Click **Next**.
The login page for the selected cloud service opens.
5. Specify your user name and password.
The QNAP Connect to Cloud Drive authorization screen appears.
6. Click **Yes** or **Allow**.
File Station connects with the cloud service.
7. Specify a connection name.
8. Click **Apply**.
File Station mounts the cloud drive.

Mounting a Remote Device

1. Open File Station.
2. Click **Remote Mount** and then select **Create remote mount**.
The **Create remote mount** window opens.
3. Under **Remote device network protocol**, select one of the following options and then click **Next**.

Option	Tasks
Auto Search	a. Select a device from the list or manually specify the IP address.

	File Station displays the network information of the detected devices if the information is available. - Specify the device user name and password. - Click Next. - Select the network protocol and then click Next. - Select the destination folder. - Specify the connection name. - Click Create Now.
CIFS/SMB	- Specify the host name or IP address, or click Find the NAS on the local network. File Station displays the network information of the detected devices if the information is available. - Optional: Specify the port number. - Specify the device user name and password. - Select the destination folder. - Specify the connection name. - Optional: Select Support multimedia playback and thumbnail display. - Click Create.
FTP	- Optional: Select a code page. - Specify the host name or IP address, or click  to search a device on the local network. File Station displays the available network information of the detected devices. - Optional: Specify the port number. - Specify the device user name and password.  Note To access the device anonymously, select Anonymous login. - Select a destination folder. - Specify the connection name. - Click Create.
WebDav	 Note To mount a remote device via WebDav, you must install the Connect to Cloud Drive app from App Center. Using a QNAP device as the remote host: Specify the host name or IP address.

	b. Specify the port number. c. Specify the device username and password. d. Select the destination folder. e. Specify the connection name. f. Click Create. Using a non-QNAP device as the remote host: a. Specify the server URL. b. Specify the device username and password. c. Specify the connection name. d. Click Create.
--	---

Viewing Recent Connection Records

1. Open File Station.
2. Click **Remote Mount** and then select **Connection record**.
The **Recent connection record** window opens and displays the information of recent connections.



Note

File Station only retains the 200 most recent connections.

3. Click **Close**.

Viewing Current Connection Status

1. Open File Station.
2. Click **Remote Mount** and then select **Current connection status**.
The **Current connection status** window opens and displays the information of the current connections.
3. Click **Close**.

9. License Center

License Center lets you monitor and manage the licenses of your applications running on your NAS. Through License Center, you can perform the following actions.

- Purchase licenses through the application's built-in License Store
- Activate and deactivate licenses either manually or automatically, and either offline or through myQNAPcloud Link
- Delete licenses
- Recover licenses if you recently reinitialized your NAS
- Transfer licenses purchased from the old QNAP License Store to the new License Store

Buying Licenses Using QNAP ID

Before buying a license, ensure the following.

- The application is already installed on your NAS.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **License Store**.
3. Select a currency.
4. Locate the product on the list, and then click **Buy**.
The license details appear.
5. Review the details, and then click **Next**.
The **Authentication** dialog box appears.
6. Specify your QNAP ID password.
7. Click **Next**.
The product window appears.
8. Select the item you want to buy, and then review the price.
9. Read and agree to the terms of service and product agreement.
10. Click **Checkout**.
The purchase summary page appears in your web browser.
11. Review the details, and then click **Buy Now**.
The secure PayPal browser window appears.
12. Select a payment method.

Payment Method	Description
Credit or debit card	Specify your payment information, including your card details, billing address, and contact information.
PayPal	Use your existing PayPal account or create a new one.

13. Click **Pay Now.**

The payment confirmation window appears.

14. Optional: Review the license details, and then click **Activate Now.**

The license is activated.

**Tip**

You can activate licenses at a later time. For details, see [License Activation](#).

License Activation

You can activate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses bought through License Center are stored in your QNAP ID account, and can be accessed through both License Center and the online License Store . To activate this type of license, see Activating a License Using QNAP ID .
Using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. You can use product keys to activate licenses in License Center. For details, see Activating a License Using a Product or License Key .
Using a license key	You can generate the 25-character license key after purchasing licenses through the QNAP License Store . For details, see Generating a License Key . You can use license keys to activate licenses in License Center. For details, see Activating a License Using a Product or License Key . License details for licenses activated using license keys are not displayed on the QNAP License Store.
Using a product authorization key (PAK)	The 24-character PAK is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you are using NAS devices running QTS version 4.3.4.0435 or older, use PAKs to activate licenses through App Center. If you are using NAS devices running QTS version 4.3.4.0483 or later, you can transfer PAKs purchased from the Old QNAP License Store to NAS devices. For details, see Activating a License Using a PAK .
Offline	Use this method when the NAS is not connected to the internet. For details, see Activating a License Offline .

Activating a License Using QNAP ID

Before activating your license, ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.

2. Go to **My Licenses**.
3. Click **Add**.
The **License Activation** window appears.
4. Select a license from the list.
5. Click **Add**.
License Center activates the license.
A confirmation message appears.
6. Click **Close**.
The license appears on the list of active licenses.

Activating a License Using a Product or License Key

Before activating your license using a product or license key, ensure the following.

- Your NAS is connected to the internet.
 - You are signed in to myQNAPcloud.
1. Open License Center.
 2. Go to **My Licenses**.
 3. Click **Add**.
The **License Activation** window appears.
 4. Click **manually activate a license**.
 5. Select **Use a product or license key**.
 6. Click **Next**.
 7. Specify the key.

Key	Description
Product key	The product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package.
License key	Users can generate a license key from the QNAP Store. For details, see Generating a License Key .

8. Read and agree to the terms of service.
9. Click **Activate**.
A notification message appears.
10. Click **Activate**.
License Center activates the license.
A confirmation message appears.
11. Click **Close**.
The license appears on the list of active licenses.

Generating a License Key

1. Open your web browser.

2. Go to <https://license.qnap.com>.
3. Sign in with your QNAP ID.
4. Go to **My Licenses**.
5. From the list of licenses, select the license you want to generate a key for.
6. In the table below, click **Activation and Installation > Activate on QTS** .
The **Activate License** window appears.
7. Select **Activate using the license key**.
8. Click **Next**.
License Store generates the license key.
9. Click  .
Your system copies the license.
10. Click **Done**.

Activating a License Using a PAK

Before activating a license using a product authorization key (PAK), ensure the following.

- Your NAS is connected to the internet.
 - You are signed in to myQNAPcloud.
1. Open License Center.
 2. Go to **My Licenses**.
 3. Click **Add**.
The **License Activation** window appears.
 4. Click **manually activate a license**.
 5. Select **Use product authorization key (PAK)**.
 6. Click **Next**.
 7. Specify the PAK.
 8. Click **Next**.
License Center transfers and activates the license.
A confirmation message appears.
 9. Click **Close**.
The license appears on the list of active licenses.

Activating a License Offline

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Add**.
The **License Activation** window appears.

4. Click **manually activate a license**.
5. Select **Offline Activation**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
8. Read and agree to the terms of service.
9. Click **Next**.
10. Read the instructions, and then click **Go to License Store**.
Your web browser opens the **QNAP License Store**.
11. Sign in with your QNAP ID.
12. Go to **My Licenses**.
13. From the list of licenses, select the license you want to activate.
14. In the table below, click **Activation and Installation**.
The license activation details appear.
15. Click **Activate on QTS**.
The **Activate License** dialog box appears.
16. Select **Offline Activation**.
17. Click **Next**.
18. Click **Browse**.
The file browser appears.
19. Locate and select the DIF from your computer.
20. Click **Upload**.
License Store activates the license.
A confirmation message appears.
21. Click **Download**.
The **QNAP License Store** downloads the license install file (LIF) to your computer.
22. Click **Done**.
23. Go back to License Center.
24. In the **License Activation** window, click **Next**.
25. Click **Browse Files**.
The file browser appears.
26. Locate and select the LIF from your computer.
27. Click **Next**.
License Center uploads the LIF and displays the license summary.
28. Click **Activate**.
The license appears on the list of active licenses.

License Deactivation

You can deactivate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses bought through License Center are stored in your QNAP ID account, and can be accessed through both License Center and the online License Store . To deactivate this type of license, see Deactivating a License Using QNAP ID .
Offline	Use this method when the NAS is not connected to the internet. For details, see Deactivating a License Offline .

Deactivating a License Using QNAP ID

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to deactivate, and then click .
The **License Deactivation** window appears.
4. Select **Use QNAP ID**.
5. Read and acknowledge the warning.
6. Click **Next**.
License Center deactivates the license.
A confirmation message appears.
7. Click **Close**.
License Center removes the license from the list of active licenses.

Deactivating a License Offline

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to deactivate, and then click .
The **License Deactivation** window appears.
4. Select **Offline Deactivation**.
5. Read and acknowledge the warning.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
License Center downloads the license uninstall file (LUF) to your computer.
8. Click **Next**.
9. Read the instructions, and then click **Finish**.
10. Open your web browser.

11. Go to <https://license.qnap.com>.
12. Sign in with your QNAP ID.
13. Go to **My Licenses**.
14. From the list of licenses, select the license you want to deactivate.
15. In the table below, click **Activation and Installation**.
The license activation details appear.
16. Under **Advanced Options**, click .
The **Deactivate License** window appears.
17. Click **Offline Deactivation**.
18. Click **Browse**.
The file browser appears.
19. Locate and select the LUF from your computer.
20. Click **Upload**.
License Store deactivates the license.
A confirmation message appears.
21. Click **Done**.

**Tip**

If the license is still listed in **My Licenses**, click  to remove it from the list. If the license has not yet expired, this action does not permanently delete the license from License Center.

License Extension

License Center will notify you 30 days before any of your subscription-based licenses expire. You can extend your QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses bought through License Center are stored in your QNAP ID account, and can be accessed through both License Center and the online License Store . If you have an existing valid, unused subscription-based license in License Center, you can use this to extend your expiring license. For details, see Extending a License Using QNAP ID .
Offline using an unused license	If you have a valid, unused subscription-based license and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using an Unused License .
Offline using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you have a valid, unused product key for a subscription-based license, and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using a Product Key .

Activation Method	Description
Purchasing a new license on the QNAP License Store	You can purchase a new subscription-based license from the QNAP License Store, and then use it to extend your expiring license. For details, see Extending a License by Purchasing Online .

Extending a License Using QNAP ID

Before extending licenses, ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.
- You have an existing valid, unused subscription-based license.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Select an unused license.



Warning

License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

5. Click **Extend**.
License Center extends the license.
A confirmation message appears.
6. Click **Close**.

Extending a License Offline Using an Unused License

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Read the instructions, and then click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
5. Read and agree to the terms of service.

6. Click **Next**.
7. Read the instructions, and then click **Go to License Store**.
Your web browser opens the QNAP License Store.
8. Sign in with your QNAP ID.
9. Go to **My Licenses**.
10. From the list of licenses, select the license you want to activate.
11. In the table below, click **Activation and Installation**.
The license activation details appear.
12. Click **Extend on QTS**.
The **Extend License** window appears.
13. Select **Use an unused license**, and then click **Next**.
The list of unused licenses appears.
14. Select an unused license.

**Warning**

License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

15. Click **Next**.
16. Click **Browse**.
The file browser appears.
17. Locate and select the DIF from your computer.
18. Click **Upload**.
A confirmation message appears.
19. Click **Download**.
The QNAP License Store downloads the license install file (LIF) to your computer.
20. Click **Done**.
21. Go back to License Center.
22. In the **License Extension** window, click **Next**.
23. Click **Browse Files**.
The file browser appears.
24. Locate and select the LIF from your computer.
25. Click **Next**.
License Center uploads the LIF and displays the license summary.
26. Click **Extend**.
A confirmation message appears.
27. Click **Close**.
The license appears on the list of active licenses.

Extending a License Offline Using a Product Key

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Read the instructions, and then click **Download**.
A notification message appears.
5. Click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
6. Read and agree to the terms of service.
7. Click **Next**.
8. Read the instructions, and then click **Go to License Store**.
Your web browser opens the QNAP License Store.
9. Sign in with your QNAP ID.
10. Go to **My Licenses**.
11. From the list of licenses, select the license you want to activate.
12. In the table below, click **Activation and Installation**.
The license activation details appear.
13. Click **Extend on QTS**.
The **Extend License** window appears.
14. Select **Use a product key**, and then click **Next**.
15. Specify the product key.
16. Click **Next**.
A confirmation message appears.
17. Click **Download**.
The QNAP License Store downloads the license install file (LIF) to your computer.
18. Click **Done**.
19. Go back to License Center.
20. In the **License Extension** window, click **Next**.
21. Click **Browse Files**.
The file browser appears.
22. Locate and select the LIF from your computer.
23. Click **Next**.

License Center uploads the LIF and displays the license summary.

24. Click **Extend**.
A confirmation message appears.
25. Click **Close**.
The license appears on the list of active licenses.

Extending a License by Purchasing Online

Before extending licenses, ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Click **manually extend a license**.
5. Select **Purchase online**.
6. Click **Next**.
The **Authentication** dialog box appears.
7. Specify your QNAP ID password.
8. Click **Next**.
The product window appears.
9. Select the item you want to buy, and then review the price.
10. Read and agree to the terms of service and product agreement.
11. Click **Checkout**.
The purchase summary page appears in your web browser.
12. Review the details, and then click **Buy Now**.
The secure PayPal browser window appears.
13. Select a payment method.

Payment Method	Description
Credit or debit card	Specify your payment information, including your card details, billing address, and contact information.
PayPal	Use your existing PayPal account or create a new one.

14. Click **Pay Now**.
The license is extended.

A confirmation message appears in License Center.

15. Click **Close**.

License Management

License Center allows you to perform any of the following license management tasks. For license management tasks that are not included in this list, contact customer support through the QNAP Helpdesk.

Task	Description
Recover a license	Restoring QNAP NAS devices to factory settings causes licenses to become unavailable. To recover licenses, see Recovering Licenses .
Transfer a license to the new QNAP License Server	When upgrading older versions of QTS to QTS 4.3.4.0483 build 20180213 and above, valid PAKs purchased from the old QNAP License Store are deactivated. These PAKs are accessible on License Center and can be transferred to and activated on the new QNAP License Server. For details, see Transferring a License to the New QNAP License Server .
Delete a license	You can delete expired subscription-based licenses from the My Licenses screen. For details, see Deleting a License .

Recovering Licenses

Before recovering licenses, ensure the following.

- Your NAS is connected to the internet.
 - You are signed in to myQNAPcloud.
1. Open License Center.
 2. Go to **Recover Licenses**.
 3. Click **Get Started**.
The **License Recovery** dialog box appears.

4. Read and agree to the terms of service.

5. Click **Recover**.
License Center automatically recovers all available licenses for applications installed on your NAS.

Transferring a License to the New QNAP License Server

Before transferring licenses, ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to transfer, and then click .
A confirmation message appears.

4. Read the terms of service, and then click **Transfer & Activate**.

**Warning**

After you register a license with your current QNAP ID, it will no longer be transferable.

License Center transfers the license.
A confirmation message appears.

5. Optional: Click **QNAP License Store** to review the license details.
6. Click **Close**.

Deleting a License

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to delete, and then click .
A confirmation message appears.
4. Click **Yes**.
License Center deletes the license.

**Tip**

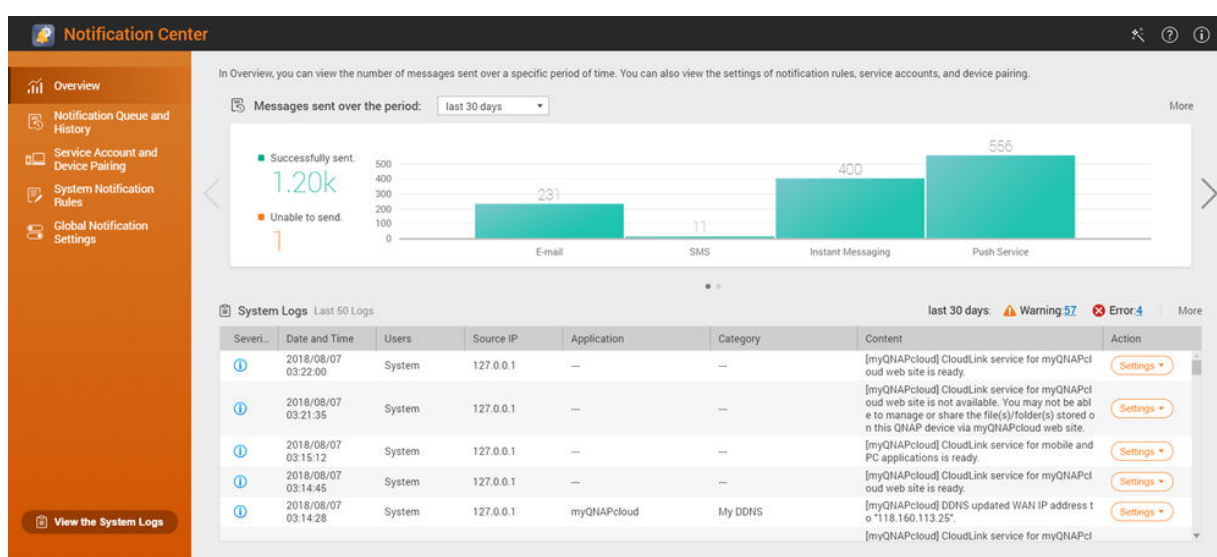
If the license has not yet expired, the license will still be listed in the **License Activation** table.

10. Notification Center

Notification Center consolidates all QTS notifications to help you monitor the status of your NAS and its applications and address potential issues more closely and promptly. You can send notifications to recipients through different channels including emails, SMS, instant messaging, and other push services. Notification Center also lets you create custom notification rules and criteria, ensuring that you receive notifications that are most relevant to your needs.

Overview

The Overview screen displays the number of notifications delivered over a specific period of time. It also displays the number of notification rules, service accounts, and paired devices you configured.



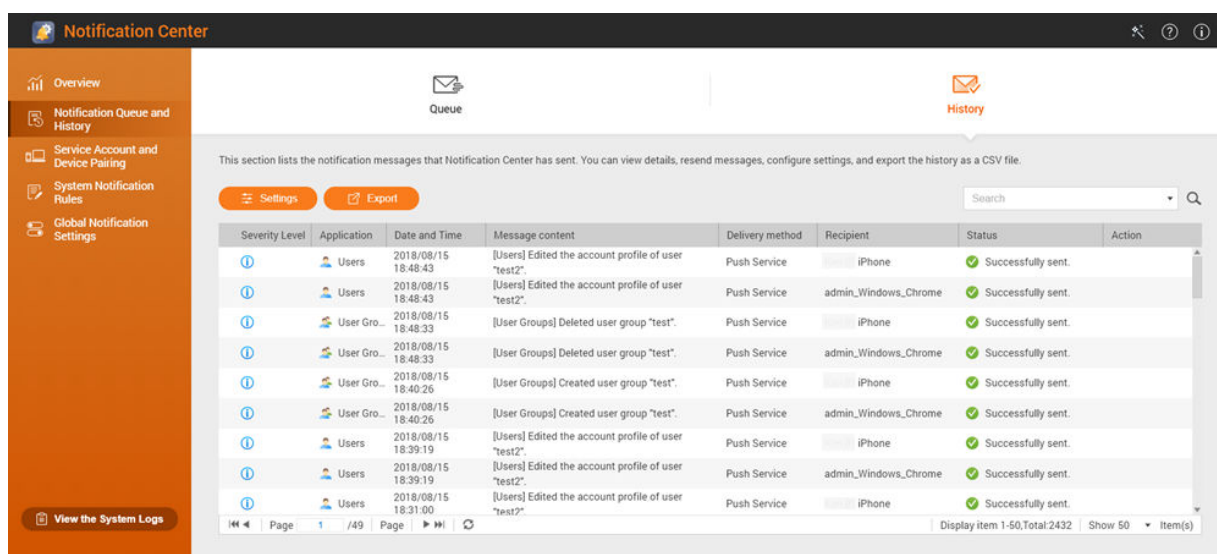
Notification Queue and History

Queue

The Queue screen displays the messages that Notification Center is going to send. The required transmission time depends on the current status of your NAS. You can remove a message from the queue before it is sent. Messages removed from the queue will not appear in the History screen.

History

The History screen displays the messages that Notification Center has sent. You can view details, resend messages, configure settings, and export the history as a CSV file. In the settings, you can specify how long your notification records are retained and where they are stored.



No.	Task	User Action
1	Export the notification message history.	Click Export . Notification Center saves the CSV file on your computer.
2	Resend the notification.	Identify the notification you want to resend, and then click  . This button only appears when Notification Center is unable to send the notification to the recipient.

Configuring History Settings

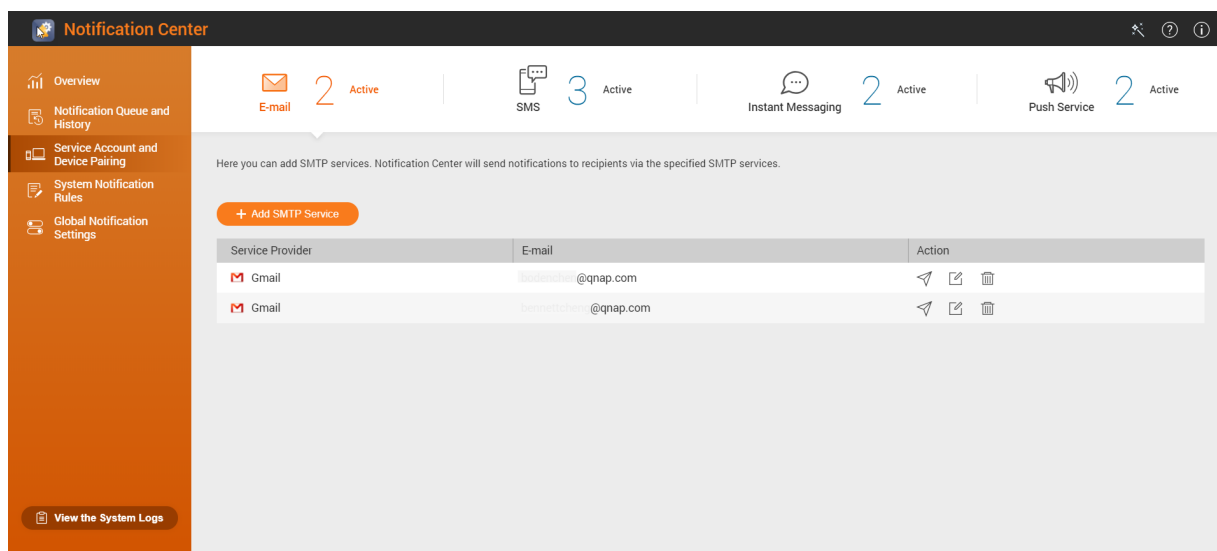
1. Open Notification Center.
2. Go to **Notification Queue and History > History**.
3. Click **Settings**.
The **Settings** window appears.
4. Configure the following information.
 - Retention period: Specify the maximum number of days Notification Center retains notification records before deleting them.
 - Notification record storage: Select whether or not you want to keep notification records in a specified local folder.
5. Click **Confirm**.
Notification Center saves your settings.

Service Account and Device Pairing

Service Account and Device Pairing allows you to configure the simple mail transfer protocol (SMTP) and short message service center (SMSC) settings so you can receive notifications through email and SMS. You can also pair your instant messaging accounts and devices with your NAS to receive notifications through instant messaging or push services.

Email Notifications

The Email screen allows you to add and view email notification recipients and configure your simple mail transfer protocol (SMTP) service settings.



Button	Task	User Action
	Send a test message to a specified recipient.	- Click  . The Send test message window appears. - Specify an email address. - Click Send.
	Edit the configurations of an existing email server.	- Click  . The Edit SMTP Service Account window appears. - Edit the settings. - Click Confirm.
	Remove an email server.	- Click  . A confirmation message appears. - Click Confirm.

Configuring an Email Notification Server

- Go to **Service Account and Device Pairing > E-mail** .
- Click **Add SMTP Service**.
The **Add SMTP Service** window appears.
- Select an email account.
- Configure the following.

Service Provider	User Action
Gmail or Outlook	- Click Add account. The email account window appears. - Specify the email address that will act as the sender for QTS notifications. A confirmation message appears. - Click Allow.
Yahoo	 Important Before configuring the Yahoo Mail settings, do the following. - Log in to your Yahoo Mail account. - Go to Help > Account Info > Account Security. - Enable Allow apps that use less secure sign in. Specify a valid Yahoo mail address and its account password.
Custom	- Specify the domain name or the IP address of your SMTP service such as <code>smtp.gmail.com</code>. - Specify the port number for the SMTP server. If you specified an SMTP port when you configured the port forwarding settings, use this port number. - Specify the email address that will act as the sender for QTS notifications. - Specify a username that contains a maximum of 128 ASCII characters. - Specify a password that contains a maximum of 128 ASCII characters. - Select one of the following secure connection options. SSL: Use SSL to secure the connection. TLS: Use TLS to secure the connection. None: Do not use a secure connection. QNAP recommends enabling a secure connection if the SMTP server supports it.
Others	Specify a valid email address and its account password.

**Tip**

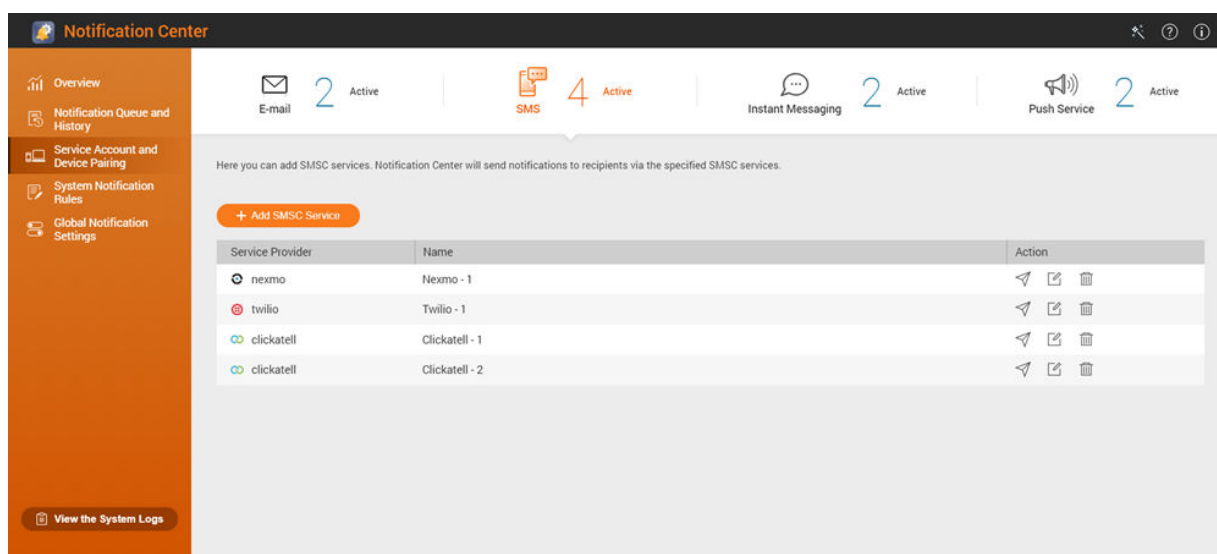
To configure multiple email servers, click **Add SMTP Service**, and then perform the previous steps.

5. Optional: Select **Set as default SMTP service account**.

6. Click **Create**.
Notification Center adds the SMTP service to the list.

SMS Notifications

The SMS screen allows you to view and configure your short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Nexmo, and Twilio.



Button	Task	User Action
	Send a test message to a specified recipient.	1. Click . The Send test message window appears. 2. Specify a country code and phone number. 3. Click Send.
	Edit the configurations of an existing SMS server.	1. Click . The Edit SMSC Service Account window appears. 2. Edit the settings. 3. Click Confirm.
	Remove an SMS server.	1. Click . A confirmation message appears. 2. Click Confirm.

Configuring an SMS Notification Server

1. Go to **Service Account and Device Pairing > SMS**.
2. Click **Add SMSC Service**.
The **Add SMSC Service** window appears.
3. Specify a service provider.
4. Specify an alias.
5. Specify the following information.

SMS Service Provider	Information
Clickatell - Communicator/Central	Clickatell username, password, and API ID

SMS Service Provider	Information
Clickatell - SMS Platform	Clickatell API key
Nexmo	Nexmo API key and secret question, and a sender name The sender name can contain a maximum of 32 characters.
Twilio	Your Twilio account SID, access token, and the Twilio-provided phone number linked to your account
Custom	- URL template text formatted according to the format specified by your SMS service provider. Use the following replaceable URL template parameters. @@UserName@@: Specify the username for this connection. @@Password@@: Specify the password for this connection. @@PhoneNumber@@: Specify the phone number where the SMS messages are sent. This parameter is required. @@Text@@: Specify the text content of the SMS message. This parameter is required.  Important You will not be able to receive SMS messages if the template text does not match the format used by your SMS service provider. - The name of the service provider. The name can contain a maximum of 32 ASCII characters. - A password. The password can contain a maximum of 32 ASCII characters.

**Tip**

To configure multiple SMS servers, click **Add SMSC Service**, and then perform the previous steps.

6.



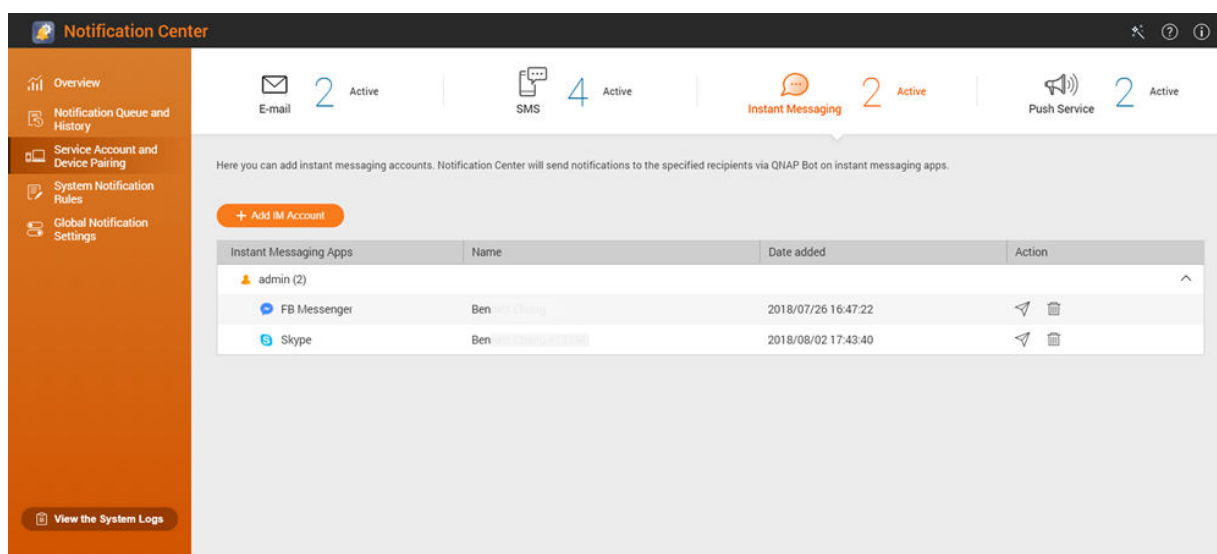
The SMS server sends a test message.

7. Click **Create**.

Notification Center adds the SMTP service to the list.

Instant Messaging Notifications

The Instant Messaging screen allows you to pair Notification Center with instant messaging accounts such as Skype and Facebook Messenger. Notification Center sends notifications to the specified recipients through QBot, the QNAP instant messaging bot account.



Button	Task	User Action
	Send a test message.	Click .
	Unpair from and remove the instant messaging account.	- Click . A confirmation message appears. - Click Confirm.

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Skype account.
- Skype is installed on your device.

1. Go to **Service Account and Device Pairing > Instant Messaging**.
2. Click **Add IM Account**.
The **Notification IM Wizard** appears.
3. Select Skype.
The **Add Bot to Contacts** window appears.
4. Log in to the Skype account you want to pair.
Skype adds QNAP Bot as a contact.
5. Close the **Add Bot to Contacts** window.
6. Click **Next**.
A verification code appears.
7. On Skype, enter the verification code.
Notification Center verifies and pairs with the Skype account.

8. Click **Finish**.

Notification Center adds the Skype account to the list.

Pairing Notification Center with Facebook Messenger

Before configuring instant messaging (IM) notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Facebook Messenger account.

1. Go to **Service Account and Device Pairing > Instant Messaging**.

2. Click **Add IM Account**.

The **Notification IM Wizard** appears.

3. Select Facebook Messenger.

The **Add Bot to Contacts** window appears.

4. Log in to the Facebook Messenger account you want to pair.

Facebook Messenger adds QNAP Bot as a contact.

5. Click **Get Started**.

A verification code appears on the **Notification IM Wizard**.

6. On Facebook Messenger, enter the verification code.

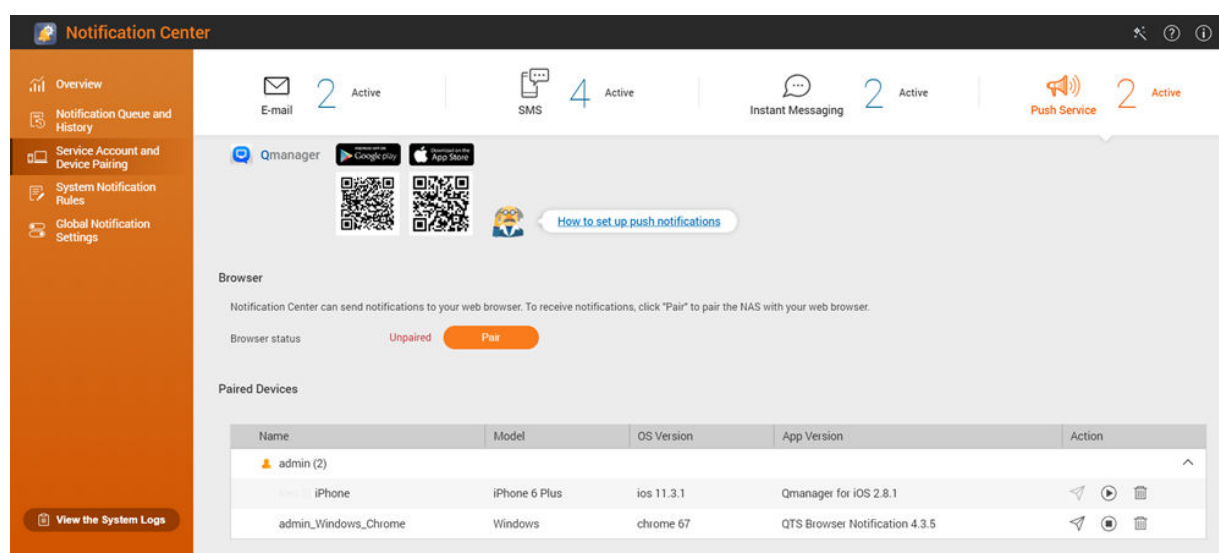
Notification Center verifies and pairs with the Facebook Messenger account.

7. Click **Finish**.

Notification Center adds the Facebook Messenger account to the list.

Push Notifications

The Push Service screen allows you to configure push services for web browsers and mobile devices.



Button	Task	User Action
	Send a test message.	Click  .
	Start sending push notifications to the device or browser.	Click  .
	Stop sending push notifications to the device or browser.	Click  .
	Unpair and remove the device or browser.	- Click . A confirmation message appears. - Click Confirm.

Pairing Notification Center with a Mobile Device

Before pairing, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- Qmanager is installed on the mobile device.
- Your NAS is added in Qmanager.

1. Open Qmanager on the mobile device.
2. Perform one of the following.

Pairing Option	User Action
Automatic pairing	a. From the device list, tap the NAS you want to pair. A confirmation message appears. b. Tap Confirm.
Manual pairing	a. Identify your NAS from the device list, and then tap . The device settings screen appears. b. Select Push notifications. c. Tap Save. A confirmation message appears. d. Tap Confirm.

Notification Center pairs with the mobile device.

3. In Notification Center, go to **Service Account and Device Pairing > Push Service**.
4. Verify that the mobile device appears in the list of paired devices.

Pairing Notification Center with a Web Browser

Before pairing, ensure the following.

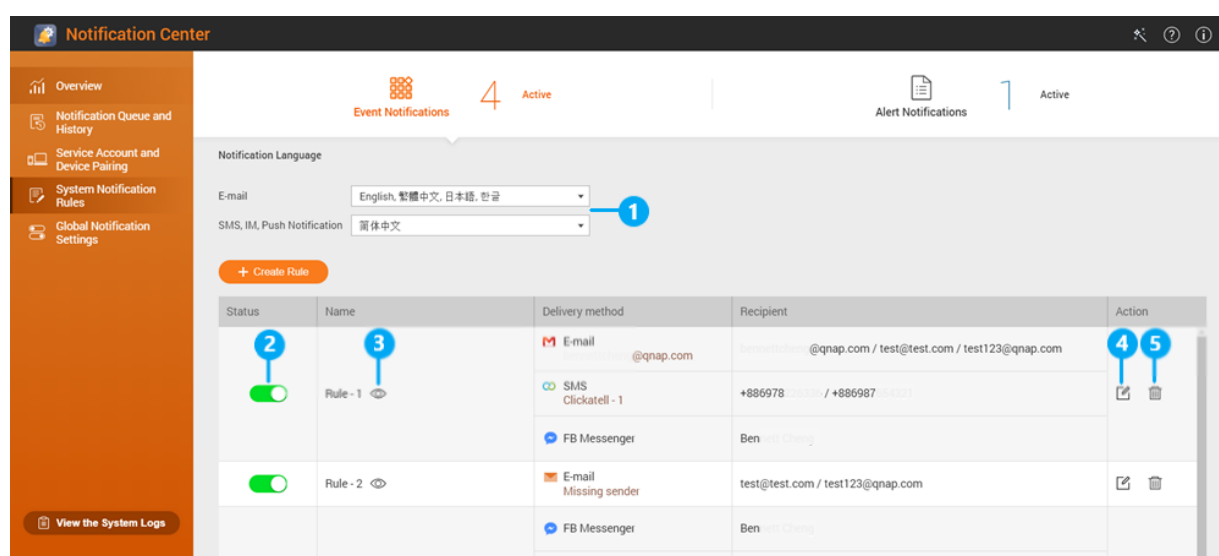
- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers: Google Chrome, Internet Explorer, Firefox, or Safari.

1. Go to **Service Account and Device Pairing > Push Service**.
2. Under Browser, click **Pair**.
Notification Center pairs with your current browser.
The browser appears in the list of paired devices.
3. Change your browser name.
 - a. Beside your browser name, click .
 - b. Specify a browser name.
The field accepts a maximum of 127 ASCII characters.
 - c. Press ENTER.
Notification Center saves your browser name.

System Notification Rules

Event Notifications

You can create custom rules and select applications and features that you want to receive event notifications from. You can also specify the message type, keywords, and time range to further define notification types or narrow the scope. Notification Center supports sending event notifications in multiple languages and provides four delivery methods to meet your different needs, including emails, SMS, instant messaging, and push services.



No.	Task	User Action
1	Specify a notification language.	1. Select one or more languages for email notifications. 2. Select a language for SMS, IM, and push notifications.
2	Enable or disable the rule.	Click  .

No.	Task	User Action
3	Preview the rule settings.	1. Click . The Event Notifications window appears. 2. Review the settings, and then click Close.
4	Edit the rule.	1. Click . The Edit Rule for Event Notifications window appears. 2. Edit the settings. 3. Click Confirm.
5	Delete the rule.	1. Click . A confirmation message appears. 2. Click Confirm.

Creating an Event Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. Go to **System Notification Rules > Event Notifications**.
2. Click **Create Rule**.
The **Create event notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.



Tip

To select all events, select **Select all**.

To display only the events for a specific application or service, select the item from the **Displayed Items** drop-down menu.

5. Click **Next**.
6. Select a security level.

Security Level	Description
Information	Information messages inform users of changes in the NAS settings or its applications.
Warning	Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features.

7. Specify a keyword filter.

Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.



Important

The event notification filter only accepts keywords that are in English or in any of the languages specified on the **Event Notifications** screen.

8. Specify a time range when you want to receive notifications.
9. Click **Next**.
10. Select a delivery method.
11. Configure the sender information.

Method	User Action
Email	a. Select an SMTP server.  Tip To add an SMTP server, see Configuring an Email Notification Server. b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive. c. Optional: Select Send email as plain text.
SMS	Select an SMSC server.  Note To add an SMSC server, see Configuring an SMS Notification Server.
Instant Messaging or Push Service	Notification Center automatically assigns Qbot.

12. Configure the recipient information.

Method	User Action
Email	a. Click Select NAS User. The Select NAS User window appears. b. Select one or more NAS users. c. Click Finish. The Select NAS User window closes.  Tip • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click .
SMS	a. Click Select NAS User. The Select NAS User window appears. b. Select one or more NAS users. c. Click Finish. The Select NAS User window closes. d. Select a country code for each recipient.  Tip • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click .
Instant Messaging	Select one or more recipients.  Tip To add instant messaging notification recipients, see the following topics: • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	Select one or more recipients.  Tip To add push notification recipients, see the following topics: • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

13. Optional: Click  to send a test message.

14. Optional: Click **Add Pair** to create a new pair.

15. Click **Next**.

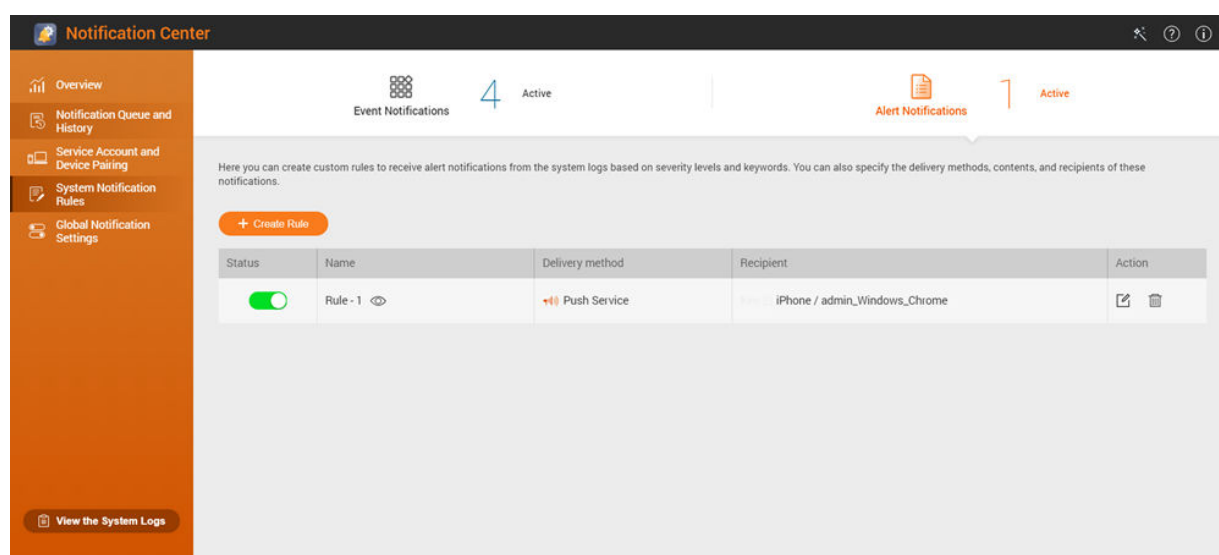
16. Verify the rule settings.

17. Click **Finish**.

Notification Center displays the new rule on the **Event Notifications** screen.

Alert Notifications

You can create custom rules to receive alert notifications from the System Logs based on the notification type and keywords. You can also specify the delivery methods, contents, and recipients of these notifications.



Button	Task	User Action
	Enable or disable the rule.	Click .
	Preview the rule settings.	- Click . The Alert Notifications window appears. - Review the settings, and then click Close.
	Edit the rule.	- Click . The Edit Rule for Alert Notifications window appears. - Edit the settings. - Click Confirm.
	Unpair from and remove the device or browser.	- Click . A confirmation message appears. - Click Confirm.

Creating an Alert Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

- Go to **System Notification Rules > Alert Notifications**.

2. Click **Create Rule**.
The **Create alert notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.
 - a. Select a security level.

Security Level	Description
Information	Information messages inform users of changes in the NAS settings or its applications.
Warning	Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features.

- b. Specify a keyword filter.

Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.



Important

The alert notification filter only accepts keywords that are in English.

5. Specify a time range when you want to receive notifications.
6. Specify a notification message threshold.
7. Click **Next**.
8. Select a delivery method.
9. Configure the sender information.

Method	User Action
Email	a. Select an SMTP server.  Tip To add an SMTP server, see Configuring an Email Notification Server. b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive. c. Optional: Select Send email as plain text.
SMS	Select an SMSC server.  Note To add an SMSC server, see Configuring an SMS Notification Server.
Instant Messaging or Push Service	Notification Center automatically assigns Qbot.

10. Configure the recipient information.

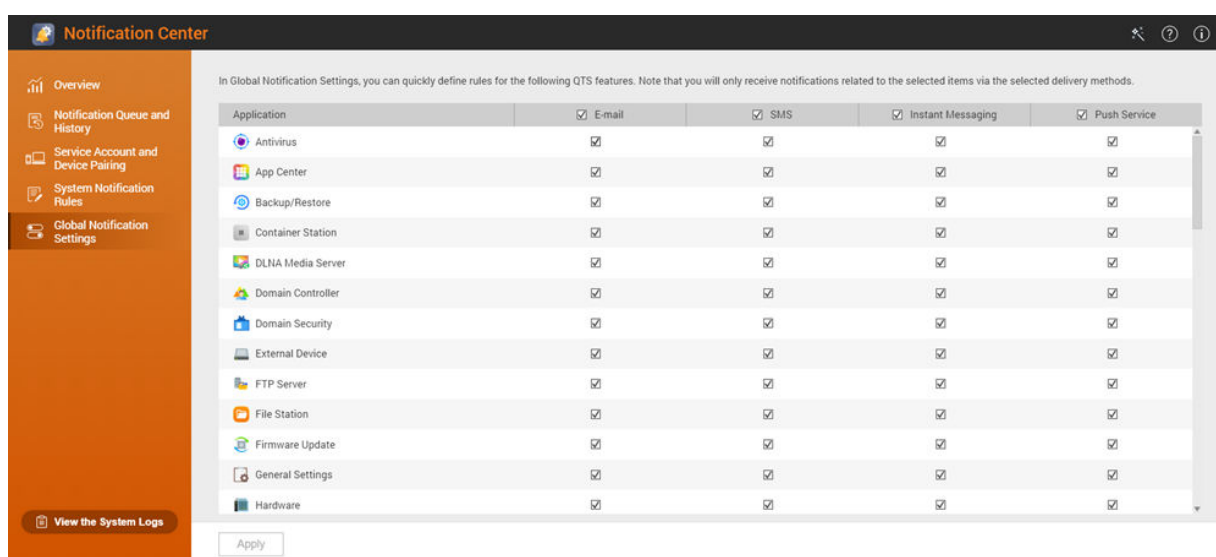
Method	User Action
Email	a. Click Select NAS User. The Select NAS User window appears. b. Select one or more NAS users. c. Click Finish. The Select NAS User window closes.  Tip • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click .
SMS	a. Click Select NAS User. The Select NAS User window appears. b. Select one or more NAS users. c. Click Finish. The Select NAS User window closes. d. Select a country code for each recipient.  Tip • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click .

Method	User Action
Instant Messaging	Select one or more recipients.  Tip To add instant messaging notification recipients, see the following topics: • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	Select one or more recipients.  Tip To add push notification recipients, see the following topics: • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

11. Optional: Click  to send a test message.
12. Optional: Click **Add Pair** to create a new pair.
13. Click **Next**.
14. Verify the rule settings.
15. Click **Finish**.
Notification Center displays the new rule on the **Alert Notifications** screen.

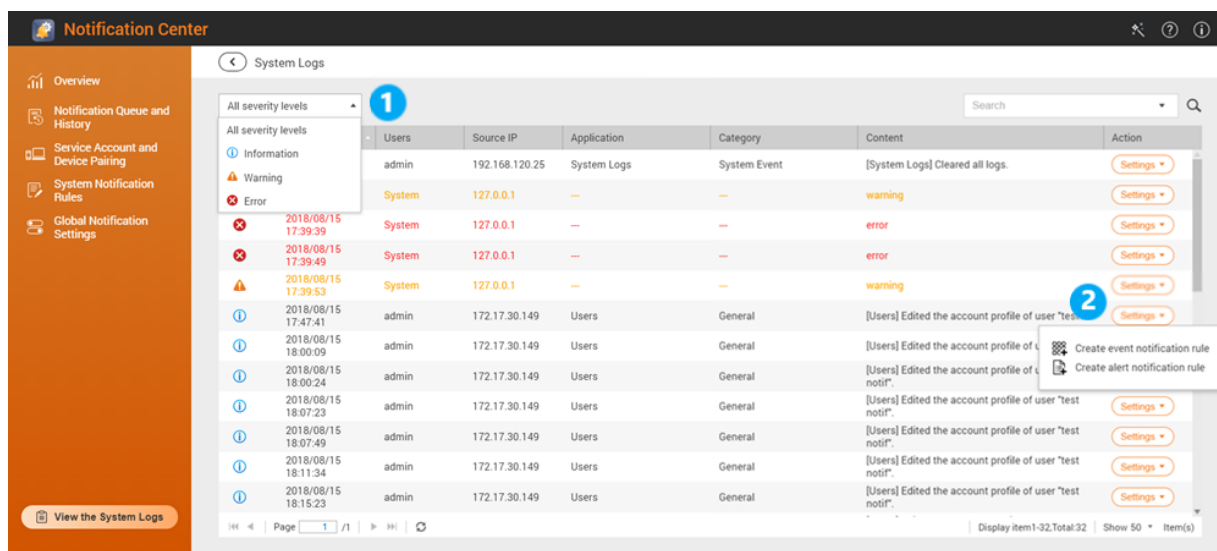
Global Notification Settings

The Global Notification Settings screen allows you to quickly define global notification rules. From the list, you can select or deselect, and then apply the delivery methods for each QTS feature or application. Users only receive notifications related to the selected features through their selected delivery methods.



System Logs

The System Logs screen displays all system events on the NAS. On this screen, you can sort and filter the logs or create notification rules based on existing logs.



No.	Task	User Action
1	Filter system logs	Select a security level.
2	Create a notification rule	1. Click Settings. 2. Select one of the following options. • Create event notification rule • Create alert notification rule The Create notification rule window appears. 3. Select one of the following options. • Add as a new rule • Add to an existing rule 4. Click Confirm. Tip To add or edit notification rules, see the following topics: • Creating an Event Notification Rule • Creating an Alert Notification Rule

11. SSD Profiling Tool

SSD Profiling Tool controls the creation and execution of SSD over-provisioning tests. These tests help determine the optimum amount of SSD over-provisioning to set when creating an SSD RAID group.

SSD Over-Provisioning

When an SSD is full, the disk's firmware frees up space in a process called garbage collection. Garbage collection results in an effect called write amplification, which reduces the lifespan and random write performance of the SSD. Write amplification can be reduced by over-provisioning, which means reserving space on the disk for garbage collection. Most SSDs are manufactured with 7% or more of their capacity reserved for over-provisioning.

SSD Extra Over-Provisioning

SSD Extra Over-Provisioning enables to you reserve additional space for over-provisioning at the RAID level when creating an SSD RAID group in QTS. Reserving extra space can increase the consistent random write performance and lifespan of the SSD group.



Important

- Space reserved for SSD Extra Over-Provisioning cannot be used for data storage. The total storage capacity of the SSD RAID group will be reduced by the specified amount.
- SSD Extra Over-Provisioning can only be enabled during RAID group creation.
- After creating a RAID group with SSD Extra Over-Provisioning enabled, you can disable the feature or decrease the amount of reserved space. It is not possible to increase reserved space.
- Results will vary depending on the SSD model. Enabling SSD Extra Over-Provisioning may have no effect on some SSDs.

SSD Over-Provisioning Tests

During an SSD over-provisioning test, SSD Profiling Tool first fills the SSDs with random data. It then tests the random write performance of the SSDs over several test phases, each using a different amount of over-provisioning. For example, if a test is created with a test range of 0-20% and a test interval of 5%, SSD Profiling Tool will test SSD write performance in 5 phases, with over-provisioning set to 0%, 5%, 10%, 15%, and 20%. If the random write performance of the disk is very low during any phase, SSD Profiling Tool will end the phase early and move to the next one.

Creating an SSD Over-Provisioning Test

1. Go to **SSD Profiling Tool > Review**.
2. Click **+ Create Test**.
The **Create SSD Test** wizard opens.
3. Click **Next**.
4. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

- You cannot select disks from multiple expansion units.

5. Select one or more disks.
Selecting a single SSD determines the optimum amount of over-provisioning for all SSDs of the same model and capacity. Selecting multiple SSDs determines the optimum amount of over-provisioning for that specific combination of disks and RAID type. Testing multiple disks gives more accurate results, but takes significantly longer than testing a single disk.



Warning

All data on the selected disks will be deleted.

6. Select a RAID type.
7. Click **Next**.
8. Optional: Configure the test settings.

Setting	Description
Test data size	SSD Profiling Tool writes the specified amount of test data to the SSD during each test phase. Decreasing the test data size decreases test time but gives less accurate results.
Over-provisioning test range	Specific the minimum and maximum amount of over-provisioning to test.
Test interval	Specific over-provisioning increments to test.

9. Review the estimated time required.
For multiple SSDs, the test may take more than 24 hours.



Tip

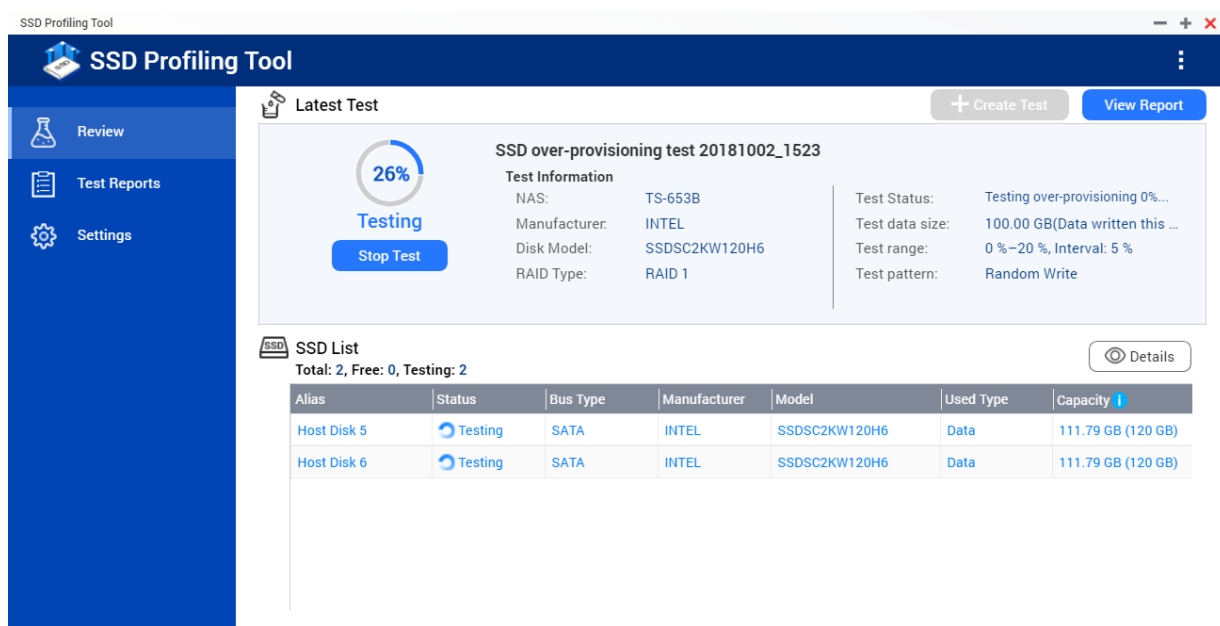
If the estimated test time is too long, reduce the test range, test interval or the test data size.

10. Click **Next**.
11. Verify the test information.
12. Click **Finish**.
A confirmation message appears.
13. Click **OK**.

SSD Profiling Tool creates and starts running the test. The test appears as a background task in QTS.

Review

This screen controls the creation and management of SSD tests and displays information about SSDs installed in the NAS.



SSD Profiling Tool

Latest Test [+ Create Test](#) [View Report](#)

SSD over-provisioning test 20181002_1523

Test Information

NAS:	TS-653B	Test Status:	Testing over-provisioning 0%...
Manufacturer:	INTEL	Test data size:	100.00 GB(Data written this ...)
Disk Model:	SSDSC2KW120H6	Test range:	0 % - 20 %, Interval: 5 %
RAID Type:	RAID 1	Test pattern:	Random Write

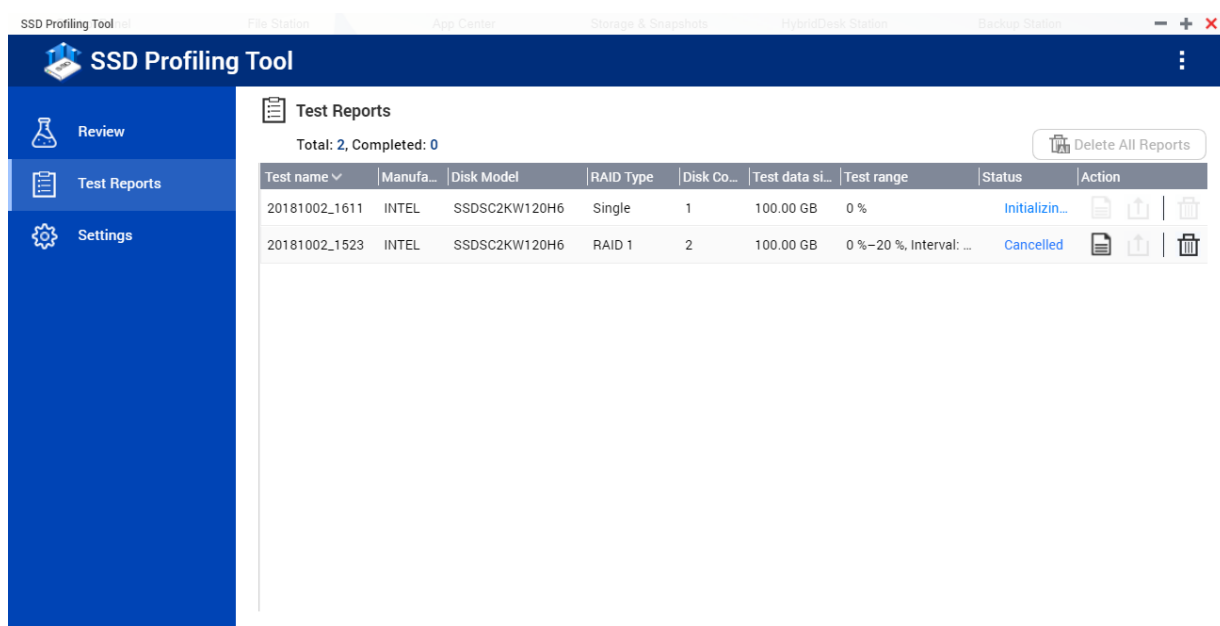
SSD List [Details](#)

Total: 2, Free: 0, Testing: 2

Alias	Status	Bus Type	Manufacturer	Model	Used Type	Capacity
Host Disk 5	Testing	SATA	INTEL	SSDSC2KW120H6	Data	111.79 GB (120 GB)
Host Disk 6	Testing	SATA	INTEL	SSDSC2KW120H6	Data	111.79 GB (120 GB)

Test Reports

On this screen you can view, export, and delete test results.



SSD Profiling Tool

Test Reports [Delete All Reports](#)

Total: 2, Completed: 0

Test name	Manufa...	Disk Model	RAID Type	Disk Co...	Test data si...	Test range	Status	Action
20181002_1611	INTEL	SSDSC2KW120H6	Single	1	100.00 GB	0 %	Initializin...	
20181002_1523	INTEL	SSDSC2KW120H6	RAID 1	2	100.00 GB	0 % - 20 %, Interval: ...	Cancelled	

Test Report Actions

Icon	Description
	Open the report in a new window.
	Download a copy of the report in XLSX format.

Icon	Description
	Delete the report.

Test Report Information

Section	Description
Test Information	View information about the NAS, the disks being tested, and the settings used in this test.
Test Result	View the test results as a graph. Choose from the following views: • IOPS / Time • IOPS / Data Written • Data Written / Time  Tip Use these graphs to compare what effect different amounts of over-provisioning had on random write speeds (IOPS).
Over-Provisioning Evaluation Results	Enter an IOPS value in Target write performance . SSD Profiling Tool will recommend the amount of over-provisioning needed to consistently achieve the target random write performance.
Test RAID Group	View information about the test SSD RAID group. Details include the RAID type, number of disks, model and capacity of each disk, and disk read/write performance.

Settings

Setting	Description
Maximum number of reports	SSD Profiling Tool retains the specified number of reports. Creating additional reports deletes the oldest ones.