QTS 5.2.x

User Guide

Document version: 1
11/07/2024

Contents

3. System Settings

4. Privilege Settings

5. Services

6. File Station

8. iSCSI & Fibre Channel

9. SSD Profiling Tool

10. Network & Virtual Switch

11. Network & File Services

15. Multimedia

16. QuLog Center

20. Console Management

1. Overview

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 helps you to manage the NAS, user accounts, data, and apps. Out of the box, QTS provides built-in features that allow you to easily store and share files. QTS also contains App Center, which offers additional downloadable applications for customizing the NAS and improving user workflows.

What's New in QTS

The following are the major new features and enhancements in the latest QTS versions.

For details, go to https://www.qnap.com/en/release-notes.

QTS 5.2.x

- To enhance device security, when you initiate restoring a device to factory default in Control Panel, you are now prompted to create a new administrator account or to retain the currently logged-in administrator account, and the default administrator account "admin" will be disabled.
- To increase device security, after restoring a device to factory default using the hardware reset button, and then logging in with the default administrator account "admin", you are now prompted to create a new administrator account and to disable the "admin" account.
- The system backup and restore functions have been upgraded with new capabilities and options. You can now restore system settings to a device of a different model running the same or a later firmware version, configure specific settings you want to restore (including general, user/group, shared folder, and network settings), install or update the applications recorded in a backup, and set up an automatic backup schedule.
- If you access your NAS primarily through a single AD domain only, you can now conveniently log in to the desktop without including the domain name in front of your username. For example, you can now enter `myusername` instead of `mydomain\myusername`. (Note: However, if you use multiple AD domains or use both local and domain user accounts to access your NAS, you should still specify the domain name when logging in with a domain user account.)
- You can now edit an iSCSI target's IQN during or after target creation (maximum 128 characters). To edit an existing target's IQN, you must first disconnect all connections to the target, and then go to **iSCSI & Fibre Channel** > **iSCSI Storage**, select the target, and click **Action Modify**.
- Users can now select what apps to install by browsing the list of installed apps on any devices connected to their QNAP IDs. To access this feature, go the the App Center, click the **Install** icon in the top-right corner, and then select **Apps Installed on All Devices**.

- Added a setting on certain device models for enabling disk auto recovery, which automatically reconnects any disks that have been unintentionally disconnected from the system. The setting can be found in **Control Panel** > **System** > **Hardware** > **General**.
- We have updated OpenSSL to version 3.0 for improved cryptographic performance, enhanced memory protection, and simplified integration with modernized APIs. Users can now experience optimized system responsiveness and better data protection.
- Added a shared folder setting which optimizes data synchronization to disks from SMB clients, thereby enhancing data integrity. You can enable the setting on a shared folder by editing its properties in **Control Panel** > **Privilege** > **Shared Folders** > **Shared Folder**, and selecting **Instant sync to disks when requested by SMB clients**.
- The ClamAV antivirus engine is now an independent application, allowing the Antivirus service to consume less memory and spend less time scanning files. Note that in order to use Antivirus, ClamAV must be installed in App Center.
- Microsoft Networking (SMB) service is now a standalone application called SMB Service, which can be updated independently. SMB Service enables remote access to your QNAP device files and folders via the Microsoft Networking (SMB) and Common Internet File System (CIFS) protocols. To enable SMB Service, you must enable Microsoft Networking in Control Panel.
- You can now calculate the size of snapshots in a volume or LUN that were taken within a specified time period. This feature can help you determine how much space you can free up by deleting a certain number of snapshots. To use this feature, open the **Snapshot Manager** window of a volume or LUN, and then click **Calculate Size**.
- In addition to media and PDF files, File Station now also supports displaying thumbnails for Microsoft Office (Word, Excel, PowerPoint) and EML files (plain text of emails). You can now quickly glance at the content of various documents even without opening the files. You can enable this support for document thumbnails in **File Station** > **Settings** > **Documents**. To use this feature, you must first install Qsirch in App Center.
- Added support for TCG Ruby SEDs.
- Implemented direct I/O in the kernel-mode SMB daemon. When the kernel-mode SMB daemon is enabled and all disks on the system device are NVMe SSDs, direct I/O enhances read and write performance.
- Improved the speed of starting and stopping applications during system startup, shutdown, and restart.

QTS initialization

Initializing QTS using Qfinder Pro

You can initialize QTS using Qfinder Pro, which is a utility designed to help you locate and manage QNAP devices on your network.

Warning
Initializing QTS deletes all data on the drives. Back up your data before proceeding.

1. Power on the NAS.
2. Connect the NAS to your local area network.
3. Run Qfinder Pro on a computer that is connected to the same local network.

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

4. Click **Next**.
   The **QNAP Warranty Service** page opens in the default web browser.
5. Click **Check warranty**.
   The **QNAP Warranty Service** window opens in a new web page.

   Important
   You can check your device warranty policy or purchase an extended warranty plan at QNAP Warranty Service.

6. Close the warranty page.
   The **Smart Installation Guide** opens in the default web browser.
7. Click **Start Smart Installation**.
8. Read the QNAP Software Terms of Use carefully.
9. Agree to the terms and conditions.
10. Click **Next**.
11. If the screen shows a different operating system, click **QTS**.

    Note
    This step is only required if the NAS supports installing more than one operating system and the default operating system for installation is not QTS.

    The NAS restarts and the smart installation screen shows QTS as the operating system to install.
12. Click **Start Smart Installation**.
13. Specify a firmware version using any of the following methods.

Methods	User Actions
Current version	Select **Current version**.

Methods	User Actions
Latest available version	**a.** Select **Latest available version**. **b.** Click **Check for Update** The system checks for the latest firmware update available for your device. If a newer version is available, the system downloads the firmware update and restarts the NAS.
Uploaded version	**a.** Select **Uploaded version**. **b.** Click **Browse**. The file upload window appears. **c.** Select a firmware file.

14. Click **Next**.
    The **Enter the NAS name and administrator's password** screen appears.
15. Specify the following information.
    - **NAS Name**: Specify a name with 1 to 14 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), but cannot end with a hyphen.
    - **Username**: Specify an administrator username that contains 1 to 32 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), multi-byte Chinese, Japanese, Korean, and Russian characters.
      The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character.

      Important
      To ensure the security of your NAS, the default "admin" account is disabled by default and cannot be used for initialization. The "admin" account can be enabled after your device is initialized, but for security reasons it is not recommended.
    - **Password**: Specify an administrator password with 1 to 64 characters. The password can contain any ASCII characters.
    - **Confirm Password**: Enter the new administrator password again.
16. Click **Next**.
    The **Set the date and time** screen appears.

17. Specify the time zone, date, and time using any of the following methods:

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

Methods	User Actions
Synchronize with computer or mobile device time	Select **Same as the computer/device time** The NAS synchronizes with the date and time of the computer or mobile device used to complete the initialization.
Enter manually	a. Select **Input Manually**. b. Specify the date and time. The NAS uses the specified date and time.
Synchronize with a time server automatically	Click **Synchronize with an Internet time server automatically**. The NAS synchronizes with the NTP server.

18. Click **Next**.
The **Configure the network settings** screen appears.

19. Configure the network settings using any of the following methods.

Methods	User Actions
Obtain an IP address automatically (DHCP)	Select **Obtain an IP address automatically (DHCP)** The system automatically detects and configures the IP address settings.
Use static IP address	a. Select **Use static IP address**. The IP address configuration page appears. b. Specify the following IP address configurations: • Interface • IP Address • Subnet Mask • Default Gateway • Primary DNS server • Secondary DNS server

20. Click **Next**.
The **Thunderbolt Connection** page appears.

> **Note**
> This page only appears if your device supports Thunderbolt. You will need to connect your device to a computer using a Thunderbolt cable.

21. Click **Next**.
    The **Summary** screen appears.
22. Review the settings.
23. Click **Apply**.
    A confirmation message appears.

    > **Warning**
    > Clicking **Initialize** deletes all data on the drive before installing QTS.

24. Click **Initialize**.

    > **Important**
    > The initialization may take several minutes to complete. Do not power off the device during the process.

QTS is initialized.

Initializing QTS using the cloud installation website

You can initialize QTS on the cloud installation website, which is designed to help you set up QNAP devices.

> **Warning**
> Initializing QTS deletes all data on the drives. Back up your data before proceeding.

1. Power on the NAS.
2. Connect the NAS to the internet.
3. Go to the QNAP Cloud Installation website using one of the following methods:
   - On your computer, go to the website dedicated to your region:
     - Global: https://install.qnap.com
     - China: https://install.qnap.com.cn
   - Or scan the QR code on the NAS using a mobile device.

   The web page lists all the uninitialized QNAP NAS devices on the local network.

4. Find your NAS from the list and then click **Initialize**.

   Tip
   If your NAS is connected to the Internet, you can also go to https://install.qnap.com/set to enter the Cloud Key printed on the NAS. This allows you to initialize the NAS even if your NAS and your computer are not on the same network.

   The installation wizard opens in the default web browser

5. Create an account or sign in to myQNAPcloud.

   Note
   You must return to this page to complete the installation after creating an account.

6. Specify the myQNAPcloud device name for the NAS.

   Note
   - The myQNAPcloud device name is used when remotely accessing the NAS.
   - For security purposes, the myQNAPcloud Link remote connection service will be disabled on your NAS after initialization. You can enable it by connecting to QTS through LAN and then installing myQNAPcloud Link.

7. Click **Next**.
   The **QNAP Warranty Service** page opens in the default web browser.

8. Click **Check warranty**.
   The **QNAP Warranty Service** window opens in a new web page.

   Important
   You can check your device warranty policy or purchase an extended warranty plan at QNAP Warranty Service.

9. Close the warranty page.
   The **Smart Installation Guide** opens in the default web browser.

10. Click **Start Smart Installation**.

11. Read the QNAP Software Terms of Use carefully.

12. Agree to the terms and conditions.

13. Click **Next**.

14. If the screen shows a different operating system, click **QTS**.

    Note

    - This step is only required if the NAS supports installing more than one operating system and the default operating system for installation is not QTS.
    - If the screen shows QuTS hero, you may need to click **Skip** first.

    The NAS restarts and the smart installation screen shows QTS as the operating system to install.

15. Click **Start Smart Installation**.

16. Specify a firmware version using any of the following methods.

Methods	User Actions
Current version	Select **Current version**.
Latest available version	**a.** Select **Latest available version**. **b.** Click **Check for Update** The system checks for the latest firmware update available for your device. If a newer version is available, the system downloads the firmware update and restarts the NAS.
Uploaded version	**a.** Select **Uploaded version**. **b.** Click **Browse**. The file upload window appears. **c.** Select a firmware file.

17. Click **Next**.
    The **Enter the NAS name and administrator's password** screen appears.

18. Specify the following information.

    - **NAS Name**: Specify a name with 1 to 14 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), but cannot end with a hyphen.
    - **Username**: Specify an administrator username that contains 1 to 32 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), multi-byte Chinese, Japanese, Korean, and Russian characters.
      The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character.

Important
To ensure the security of your NAS, the default "admin" account is disabled by default and cannot be used for initialization. The "admin" account can be enabled after your device is initialized, but for security reasons it is not recommended.

- **Password**: Specify an administrator password with 1 to 64 characters. The password can contain any ASCII characters.
- **Confirm Password**: Enter the new administrator password again.

19. Click **Next**.
    The **Set the date and time** screen appears.
20. Specify the time zone, date, and time using any of the following methods:

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

Methods	User Actions
Synchronize with computer or mobile device time	Select **Same as the computer/device time** The NAS synchronizes with the date and time of the computer or mobile device used to complete the initialization.
Enter manually	a. Select **Input Manually**. b. Specify the date and time. The NAS uses the specified date and time.
Synchronize with a time server automatically	Click **Synchronize with an Internet time server automatically**. The NAS synchronizes with the NTP server.

21. Click **Next**.
    The **Configure the network settings** screen appears.
22. Configure the network settings using any of the following methods.

Methods	User Actions
Obtain an IP address automatically (DHCP)	Select **Obtain an IP address automatically (DHCP)** The system automatically detects and configures the IP address settings.

Methods	User Actions
Use static IP address	**a.** Select **Use static IP address**. The IP address configuration page appears. **b.** Specify the following IP address configurations: • Interface • IP Address • Subnet Mask • Default Gateway • Primary DNS server • Secondary DNS server

23. Click **Next**.
    The **Thunderbolt Connection** page appears.

    Note
    This page only appears if your device supports Thunderbolt. You will need to connect your device to a computer using a Thunderbolt cable.

24. Click **Next**.
    The **Summary** screen appears.
25. Review the settings.
26. Click **Apply**.
    A confirmation message appears.

    Warning
    Clicking **Initialize** deletes all data on the drive before installing QTS.

27. Click **Initialize**.

    Important
    The initialization may take several minutes to complete. Do not power off the device during the process.

QTS is initialized.

Initializing QTS using an HDMI connection

You can initialize QTS on an HDMI display if your NAS supports HDMI.

Warning
Initializing QTS deletes all data on the drives. Back up your data before proceeding.

1. Connect an HDMI display to the NAS.
2. Connect a USB keyboard to the NAS or prepare the QNAP IR remote control (not available on all models).
3. Power on the NAS.
   The **Welcome** screen of the Smart Installation Guide appears.
4. Select **Start Smart Installation Guide**.
   The **Enter the NAS name and administrator's password** screen appears.
5. Specify the following information:
   - **NAS Name**: Specify a name with 1 to 14 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), but cannot end with a hyphen.
   - **Username**: Specify an administrator username that contains 1 to 32 characters. The name can contain letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), multi-byte Chinese, Japanese, Korean, and Russian characters.
     The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character.

     Important
     To ensure the security of your NAS, the default "admin" account is disabled by default and cannot be used for initialization. The "admin" account can be enabled after your device is initialized, but for security reasons it is not recommended.
   - **Password**: Specify an administrator password with 1 to 64 characters. The password can contain any ASCII characters.
   - **Confirm Password**: Enter the new administrator password again.
6. Click **Next**.
   The **Thunderbolt Connection** page appears.

   Note
   This page only appears if your device supports Thunderbolt. You will need to connect your device to a computer using a Thunderbolt cable.
7. Click **Next**.
   The **Summary** screen appears.
8. Review the settings.

9. Click **Next**.
   The **Confirm** screen appears.

   Warning
   Clicking **Next** deletes all data on the drive before installing QTS.

10. Click **Next**.

    Note
    The initialization may takes several minutes to complete. Do not power off the device during the process.

QTS is initialized.

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 • Login credentials of a valid user account For details, see Accessing the NAS using a browser.	• A computer 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.	• A computer 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.	• A mobile device connected to the same network as the NAS • Qmanager

Method	Description	Requirements
Explorer (Windows)	You can map a NAS shared folder as a network drive to easily access files using Explorer. For details, see the following topics. • Mapping a shared folder on a Windows computer • Mounting a shared folder using WebDAV on Windows	• A Windows computer 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, see the following topics. • Mounting a shared folder on a Mac computer • Mounting a shared folder using WebDAV on Mac	• A Mac computer 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. Optional: Log in QTS using HTTPS.
   a. Select **Secure login**.
      A confirmation message appears.
   b. Click **OK**.
      You will be redirected to the QTS HTTPS login page.

5. Choose one of the following login methods.

Method	Description
NAS account	Log in with your NAS username and password. **Tip** You can further enhance your account security with 2-step verification. For details, see 2-step verification.
QNAP ID	Log in with your QNAP ID. To use this method, you need to create a QNAP ID and link it to your NAS. For detail, see myQNAPcloud.
Azure SSO	Log in with Azure SSO. To use this method, you need to set up Azure AD Single-Sign-On. For details, see Azure Single Sign-On (SSO).

The QTS desktop appears after your successful login.

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/go/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	**a.** Tap **Add NAS manually**. **b.** Specify the following information. • Host name or IP address of the NAS • Password of the admin account **c.** Tap **Save**.
Sign in using QID	**a.** Tap **Sign in QID**. **b.** Specify the following information. • Email address that you used to create your QNAP account • Password of your QNAP account **c.** Tap **Sign in**. **d.** Locate the NAS in the list, and then tap the name or IP address.

QTS navigation

There are several methods for navigating QTS. You can navigate the operating system using the task bar, left panel, main menu, and through the desktop.

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.

No.	Element	Possible User Actions
3	**Search**	• Type keywords 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. **Tip** App or utility search results are classified into **Systems**, **Application**, and **Help**.

4	**Volume Control**	**Important**
		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.

5	**Background Tasks**	• Hover over the button to see the number of ongoing background tasks. Examples of background tasks include 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.

No.	Element	Possible User Actions
6	**External Devices**	• Hover over the button to view the number of external storage devices and the number of 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**	• Hover over the button to see the number of recent errors and warnings.
		• 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 **Event Log** window.
		• Click **More>>** to open **QuLog Center**.
		• Click **Clear All** to delete all list entries.

8	**Personal Settings**	Click the profile picture to open the **Personal Settings**.

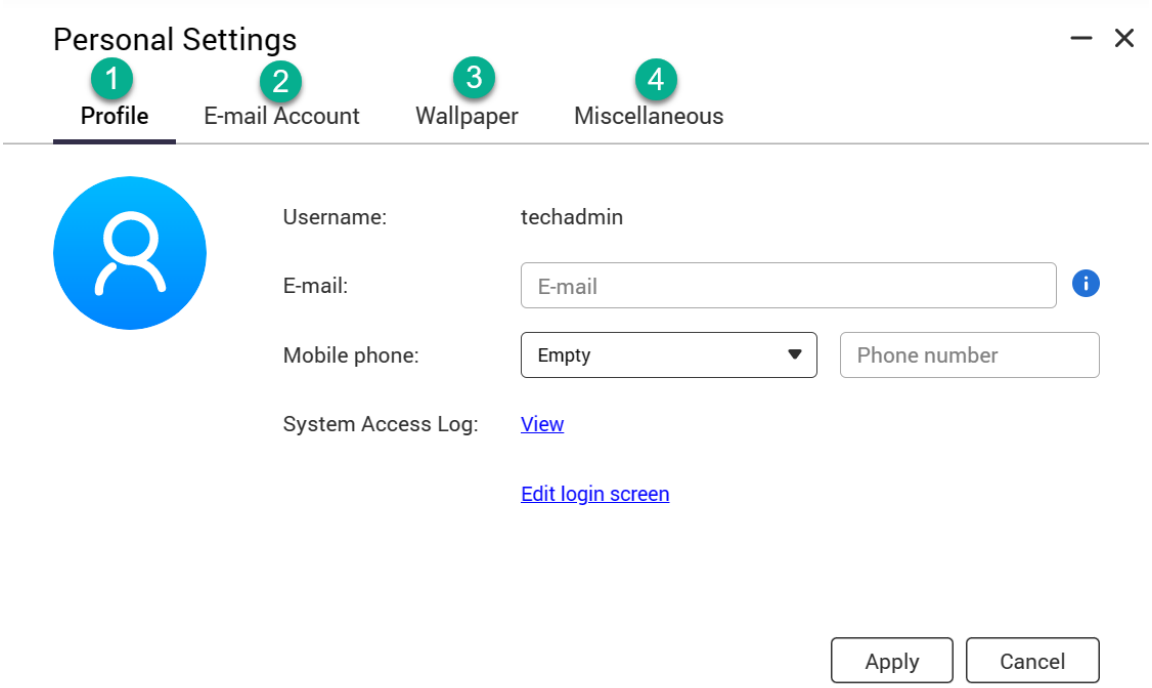
No.	Element	Possible User Actions
9	**[USER_NAME]**	Click the button to view the last login time and the following menu items: • **Language**: Opens a list of supported languages and allows you to change the language of the operating system • **Desktop Preferences**: Opens a list of display modes and allows you to select the mode based on your device type • **Personal Settings**: Open the **Personal Settings** window for configuring user settings such as user profile, email account, wallpaper, and other miscellaneous settings. • **Login and Security**: Open the **Login and Security** window for configuring settings such as password, 2-step verification, and passwordless login, and SSH Keys. • **Locate my NAS**: This makes your NAS beep or flash drive LEDs to help you locate your device. • **Sleep**: Keeps the NAS powered on but significantly reduces power consumption **Note** 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, locate the device in the list. Right click on the device and select **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
		• **Help Request**: Opens the Helpdesk window
		• **Terms of Use**: Open the **QNAP Terms and Conditions of Use** page
		• **Data & Privacy**: Opens the **QNAP Privacy Policy** page
		• **Device QR Code**: Displays a QR code that contains the essential network information of this device. You can scan this QR code with a QNAP mobile app to quickly add this device to your mobile app.
		• **About**: Displays the following information:
		  • Operating system
		  • Hardware model
		  • Operating system version
		  • Number of installed drives
		  • Number of empty drive bays
		  • System volume name

11	**Notice Board**	Display all system notifications and the Getting Started Guide for system setup.
12	**Dashboard**	Click the button to display the dashboard.
13	**myQNAPcloud/ AMIZ Cloud**	After signing in to your QNAP ID, you can click this button to go to the myQNAPcloud website or the AMIZ Cloud website, depending on your device management settings.

Personal Settings



No.	Tab	Possible User Actions

1	**Profile**	• Specify the following optional information:
		  • Profile picture
		  • Email address
		  • Phone number
		• Click **View** to display the **System Access Log** screen.
		• Click **Edit login screen** to open the **Login Screen** configuration screen in the **Control Panel** window.
		• Click **Apply** to save all changes.

2	**E-mail Account**	• Add, edit, and delete email accounts to use when sharing files. • Click **Apply** to save all changes.

No.	Tab	Possible User Actions

3	**Wallpaper**	• Perform any of the following actions:
		  • Desktop icon and font size: Choose a large or a small size for desktop icons and text fonts.
		  • Dynamic wallpaper: Specify the daytime and nighttime, then select a wallpaper pairing. The system automatically switches the wallpaper between daytime and nighttime modes at the specified time.
		  • Picture: Select from the default images or upload an image, then specify the image fill mode.
		  • Color: Select a color from the default settings or specify a color.
		• Click **Apply** to save all changes.

No.	Tab	Possible User Actions

4	**Miscel-laneous**	• 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.
		  • **Show the Dashboard button**: When enabled, QTS displays the button to show the dashboard on the taskbar.
		  • **Show the NAS time on the desktop**: When enabled, QTS displays the current NAS time, day, and date at the bottom-right 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 **Control Panel** > **System** > **System Status** > **System Information**. If disk-related issues occur, click the heading to open **Storage & Snapshots**. If PSU-related issues occur, click the heading to open **Control Panel** > **System** > **System Status** > **Hardware Information**
2	Hardware Information	• System temperature • CPU fan speed • System fan speed	Click the heading to open **Control Panel** > **System** > **System Status** > **Hardware Information**.

No.	Section	Displayed Information	User Actions
3	Resource Monitor	• CPU usage in % • Memory usage in % • Network upload and download speeds for each adapter.	Click the heading to open **Control Panel** > **System** > **Resource Monitor** > **Overview**.
4	Expansion Cards	For each expansion card: • Assignment (or "Ready" if unassigned) • Manufacturer • Model • Memory usage • GPU usage • Fan speed • Temperature	Click the heading to open **Control Panel** > **System** > **Hardware** > **Expansion Cards**.

5	Disk Health	• Number of installed disks
		• Health status of installed disks
		• Number of VJBOD disks
		• Health status of VJBOD disks
			• Click the heading to open the **Disk Health** screen in **Storage & Snapshots**.
			• 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 **Storage & Snapshots** > **Overview**.

No.	Section	Displayed Information	User Actions
6	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.
7	Online Users	• Login time • Username • Total connection time • IP address • Connection type • Client app	Click the heading to open **Control Panel** > **System** > **QuLog Center** > **Online Users**.

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

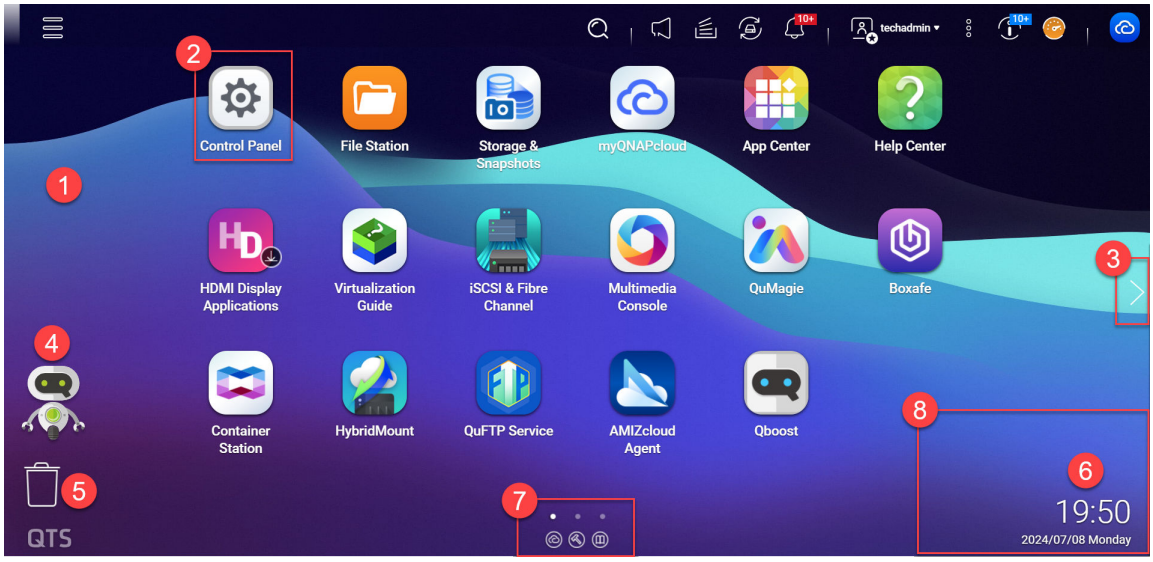
2	System	Displays a list of system utilities and other programs that enable you to manage the NAS.
		The following are the default system utilities:
		• Control Panel
		• Storage & Snapshots
		• iSCSI & Fibre Channel
		• Users
		• Network & Virtual Switch
		• myQNAPcloud
		• Resource Monitor
		• App Center
		• Help Center
		• Qboost
		• HDMI Display Applications
		Note
		This menu item only appears 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.

No.	Section	Description	Possible User Actions

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:
		• Hybrid Backup Sync 3
		• File Station
		• Helpdesk
		• License Center
		• Multimedia Console
		• Notification Center
		• QTS SSL Certificate
			• 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.

4	Search	Displays apps that meet your search criteria.	Enter keywords.

Desktop



No.	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	Each icon opens an app or a utility.
		When you install an application, QTS automatically creates a desktop shortcut. The following are the default shortcuts:
		• Control Panel
		• File Station
		• Storage & Snapshots
		• App Center
		• Help Center
		An app shortcut becomes dimmed if the app is stopped or is currently being installed, updated, removed, or migrated.
			• 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.
			Tip
			You cannot open an app when its shortcut is dimmed, but you can click a dimmed shortcut to learn more about the current status of the app.

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. You can install Qboost in the App Center.	• Click  or  to display the memory status and open the Qboost panel. • Click  or  to hide the memory status and close the Qboost panel.

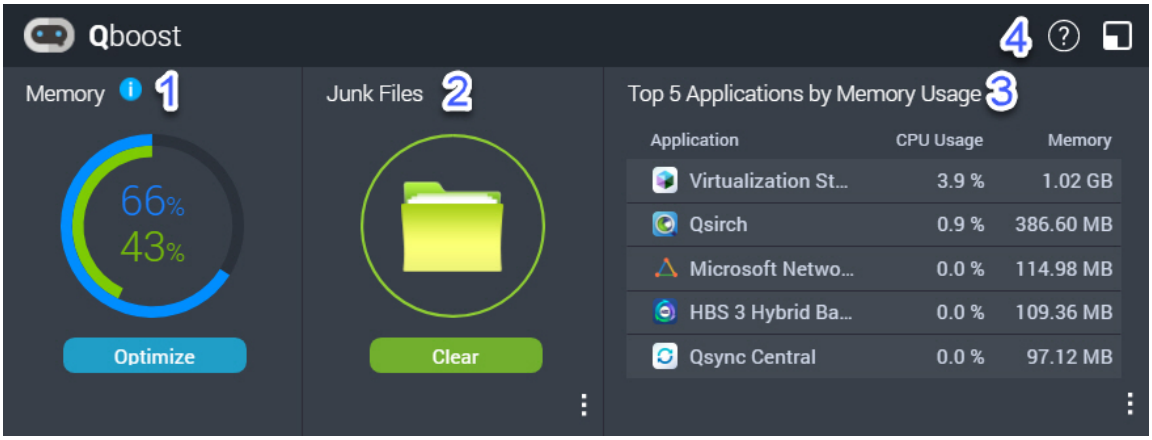
No.	Element	Description	Possible User Actions

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 system installation.	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 a new browser tab •  : Opens the download page for mobile applications and utilities •  : Provides links to the QNAP Tutorials, QNAP Forum, and Customer Service portal •  : Opens the Helpdesk utility

No.	Element	Description	Possible User Actions
8	Notifications	The system displays notifications in this area. Notifications inform the user of important system events that may require user action. If there are multiple notification groups, notices are arranged according to the notification type on a notice board. You can also view notifications in **Notice Board**. For details, see Task bar. **Tip** When you initialize QTS, the Getting Started guide will appear in notifications after installation.	Click a notification to open the corresponding utility or app.

Qboost



Qboost is a system utility that monitors and enables you to manage memory consumption. You can download the utility from App Center. It provides the following information:

No.	Section	Description	User Actions
1	Memory	A graphic showing memory usage on the NAS. • Blue: Available memory, expressed as a percentage. Available memory is the sum of free memory, buffer memory, cache memory, and other reclaimable memory. • Green: Free memory, expressed as a percentage. Free memory is memory that is currently unused and unallocated.	Click **Optimize** to clear the buffer memory (block level) and cache memory (file level). Hover the pointer over the memory widget to see the amount of available memory and free memory in MB, GB, or TB.
2	Junk Files	Junk files are unnecessary system files and files in the Recycle Bin, which consume disk space and memory.	• Click **Clear** to permanently delete junk 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.
4	Qboost taskbar	Taskbar for the Qboost widget	Click  to view the Qboost help. Click  to close the Qboost widget.

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.

Objective	Action
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.

Password management

Changing the password

Important

- The default password for the "admin" account is the Cloud Key of the device. You cannot use this default password as your new password.
- When changing your password, you are logged out of your account on all applications, browsers, and devices. You will need to log in again with your new password.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Password** tab.
4. Specify your old password.
5. Specify your new password.

   Tip
   Passwords can include up to with 64 ASCII characters or 64 bytes of UTF-8 encoded characters. QNAP recommends creating a strong password to enhance your device security.

6. Click **Apply**.

Enabling the password reset option

You can choose to send a URL and a verification code to your email address if you forgot your current password. You can then click this URL and enter the code to reset your password.

Note
To enable this feature, ensure that you have provided your personal email address in **Personal Settings** > **Profile**. The email address specified in your profile is also used for password reset.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Password** tab.
4. Enable **Send a URL and verification code to my personal email address**.
5. Click **Apply**.

Logging out of your account from multiple places

If you suspect that your account has been compromised, you can immediately log out of your account on all applications, browsers, and devices.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Password** tab.
4. Click **Log Me Out**.

2-step verification

Overview

2-step verification enhances the security of user accounts by requiring an extra verification method in addition to user passwords. To use 2-step verification, you must install one of the following authenticator applications on your mobile device.

- QNAP Authenticator
- Microsoft Authenticator
- Google Authenticator

We recommend using QNAP Authenticator, which supports all verification methods. Microsoft Authenticator and Google Authenticator only support the Security Code (TOTP) method.

Important

- You cannot enable 2-step verification and passwordless login at the same time.
- Some verification methods require the myQNAPcloud service and a QNAP ID to access the NAS via the Internet. We recommend setting up myQNAPcloud and creating a QNAP ID before enabling 2-step verification if you want to remotely access your NAS.

Supported Verification Methods

QTS supports the following four verification methods for 2-step verification. You can enable multiple verification methods, and you can choose freely from these methods upon each login.

Verification Method	Description
Security Code (TOTP)	Enter a dynamic security code generated by your authenticator app every 30 seconds. This verification method does not require a network connection. **Tip** • Security Code (TOTP) is a mandatory verification method if you enable 2-step verification. • This verification method also supports Microsoft Authenticator and Google Authenticator.
QR Code	Use your authenticator app to scan a QR code displayed on the NAS login screen.
Login Approval	Approve a login request displayed on your authenticator app.
Online Verification Code	Enter an online verification code displayed on your authenticator app.

Enabling 2-step verification with a security code (TOTP)

You can freely choose a verification method during the 2-step verification setup. Nevertheless, we recommend enabling your 2-step verification with a security code (TOTP). You can then easily enable other methods at once after completing the setup.

Important
Security Code (TOTP) is a mandatory verification method. You still need to enable Security Code as an alternative method to complete the setup even if you choose to enable 2-step verification with other methods.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **2-Step Verification** tab.
4. Specify a recovery email address.

   Tip
   This allows the system to send you messages via your email address when you cannot access your mobile device. You can choose to use the personal email address specified in your user profile as the recovery email address.

5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **Security Code (TOTP)**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.
11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and adds the NAS to the device list.
13. On your QNAP Authenticator, go to the **TOTP** tab.
    QNAP Authenticator displays a dynamic security code that is automatically renewed every 30 seconds.
14. On the NAS, enter the security code currently displayed on QNAP Authenticator.

    Tip
    QNAP Authenticator displays a security code with a space in the middle. However, you do not need to insert a space when entering a security code on the NAS.
15. Click **Verify**.
16. Click **Finish**.
    The **Verify Your Identity** window appears.
17. Enter your password to confirm this action.
18. Click **OK**.
    QTS displays a summary of your 2-step verification settings.
19. Optional: Enable more verification methods.
    - **QR Code**
    - **Login Approval**
    - **Online Verification Code**

2-Step Verification is now enabled for your account. Starting from your next login, you will need to verify your identity with a security code (or with another method) after entering your password.

Enabling 2-step verification with a QR code

Important
You must also enable the Security Code (TOTP) as an alternative verification method.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **2-Step Verification** tab.
4. Specify a recovery email address.

   Tip
   This allows the system to send you messages via your email address when you cannot access your mobile device. You can choose to use the personal email address specified in your user profile as the recovery email address.
5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **QR Code**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.
11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and adds your NAS to the device list.
13. Click **Next**.
    QTS displays a summary of your 2-step verification settings.
14. Optional: Enable more verification methods.
    - **QR Code**
    - **Login Approval**
    - **Online Verification Code**
15. Click **Next**.
    The **Verify Your Identity** window appears.
16. Enter your password to confirm this action.

17. Click **Finish**.
18. Set up Security Code (TOTP) as an alternative verification method.
    a. Use your QNAP Authenticator to scan the QR code displayed on the computer screen.
    QNAP Authenticator displays a dynamic security code that is automatically renewed every 30 seconds.
    b. On the NAS, click **Next**.
    c. On the NAS, enter the security code currently displayed on your QNAP Authenticator.
    d. Click **Verify**.
19. Click **Finish**.
    QTS displays a summary of your 2-step verification settings.

2-Step Verification is now enabled for your account. Starting from your next login, you will need to verify your identity with a QR code (or with another method) after entering your password.

Enabling 2-step verification with a login approval

Important
You must also enable the Security Code (TOTP) as an alternative verification method.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **2-Step Verification** tab.
4. Specify a recovery email address.

   Tip
   This allows the system to send you messages via your email address when you cannot access your mobile device. You can choose to use the personal email address specified in your user profile as the recovery email address.

5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **Login Approval**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.

11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and displays a verification code.
13. Verify whether QTS also displays the same verification code.
14. On QNAP Authenticator, tap **Approve** if both verification codes match.
    QTS displays a summary of your 2-step verification settings.
15. Optional: Enable more verification methods.
    - **QR Code**
    - **Login Approval**
    - **Online Verification Code**
16. Click **Next**.
    The **Verify Your Identity** window appears.
17. Enter your password to confirm this action.
18. Set up Security Code (TOTP) as an alternative verification method.
    a. Use your QNAP Authenticator to scan the QR code displayed on the computer screen.
    QNAP Authenticator displays a dynamic security code that is automatically renewed every 30 seconds.
    b. On the NAS, click **Next**.
    c. On the NAS, enter the security code currently displayed on your QNAP Authenticator.
    d. Click **Verify**.
19. Click **Finish**.
    QTS displays a summary of your 2-step verification settings.

2-Step Verification is now enabled for your account. Starting from your next login, you will need to verify your identity with a login approval (or with another method) after entering your password.

Enabling 2-step verification with an online verification code

Important
You must also enable the Security Code (TOTP) as an alternative verification method.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **2-Step Verification** tab.

4. Specify a recovery email address.

   Tip
   This allows the system to send you messages via your email address when you cannot access your mobile device. You can choose to use the personal email address specified in your user profile as the recovery email address.

5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **Online Verification Code**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.
11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and displays a verification code.
13. On the NAS, enter the verification code displayed on your QNAP Authenticator.
14. Click **Verify**.
15. Click **Next**.
    QTS displays a summary of your 2-step verification settings.
16. Optional: Enable more verification methods.
    - **QR Code**
    - **Login Approval**
    - **Online Verification Code**
17. Click **Next**.
    The **Verify Your Identity** window appears.
18. Enter your password to confirm this action.
19. Set up Security Code (TOTP) as an alternative verification method.
    a. Use your QNAP Authenticator to scan the QR code displayed on the computer screen.
       QNAP Authenticator displays a dynamic security code that is automatically renewed every 30 seconds.
    b. On the NAS, click **Next**.

c. On the NAS, enter the security code currently displayed on your QNAP Authenticator.

d. Click **Verify**.

20. Click **Finish**.
    QTS displays a summary of your 2-step verification settings.

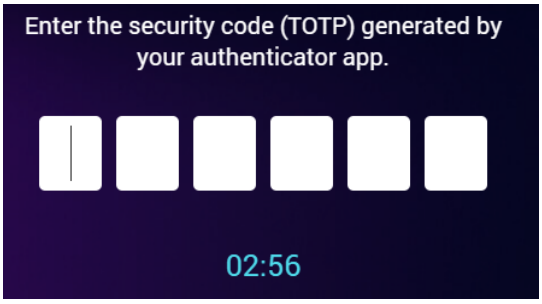
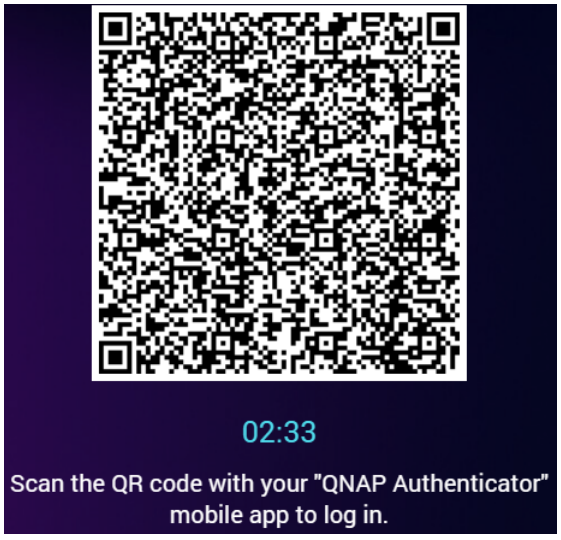
2-Step Verification is now enabled for your account. Starting from your next login, you will need to verify your identity with an online verification code (or with another method) after entering your password.

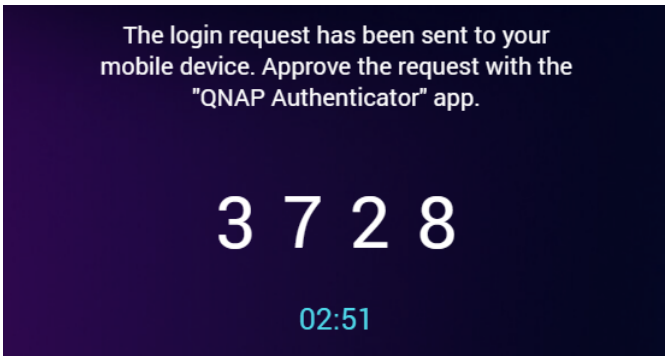
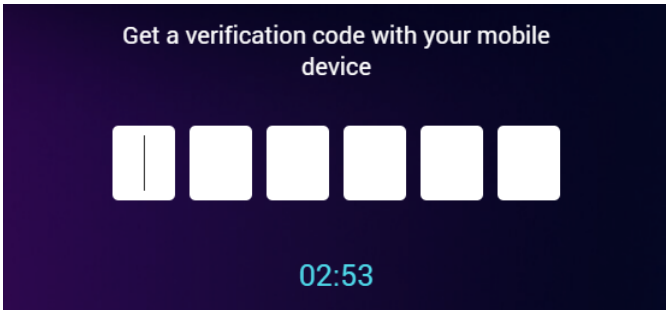
Logging in with 2-step verification

When 2-step verification is enabled, after entering your password, you must verify your identity with an extra verification method: security code (TOTP), QR code, login approval, or online verification code. These methods require your mobile device. Nevertheless, if your mobile device is not available, you can still choose to receive a verification code sent to your email address.

1. Connect to your NAS.
   The NAS displays the login screen.
2. Enter your username.
3. Click **Next**.
4. Enter your password.
5. Click **Next**.
6. Verify your identify.

> **Tip**
> You can click **Try another way** to select a different verification method.

Verification Method	User Action
Security Code (TOTP)	**a.** Open QNAP Authenticator and go to the **TOTP** tab. **b.** On the NAS, enter the security code currently displayed on QNAP Authenticator.  **c.** Click **Next**.
QR Code	Open QNAP Authenticator and scan the QR code displayed on the NAS login screen. 

Verification Method	User Action
Login Approval	**a.** Verify whether the NAS and QNAP Authenticator display the same security code.  **b.** Tap **Approve** on QNAP Authenticator.
Online Verification Code	**a.** Open QNAP Authenticator and check the verification code. **b.** On the NAS, enter the verification code.  **c.** Click **Next**.
Email	**a.** Enter the verification code sent to your email address. **b.** Click **Next**.

7. Optional: Enable **Don't verify again on this device** if you want to reduce verification frequency on this device.

After a successful verification, you are logged in to the NAS. The system displays the desktop and is ready for use.

Tip

If you cannot log in to the NAS with any of the above methods due to the unavailability of your mobile device and your email account, you can press the reset button on the NAS for 3 seconds to activate the default administrator account "admin", restore its default password (the Cloud Key of the device), and then log in to the NAS with this "admin" account. You can then disable 2-step verification for your own account in **Control Panel** > **Privilege** > **Users** > **Account Profile**. Nevertheless, after completing the setup, you should disable the "admin" account to ensure system security.

Enforcing 2-step verification

To ensure account and data security, administrators can enforce 2-step verification on specific users or groups. Once 2-step verification is enforced, users must complete the verification setup upon their next login before proceeding to any other operations.

Note

Users with the System Management or Access Management delegated role can edit 2-step verification settings on anyone except the following users and groups:

- Their own user accounts and their own groups
- Users in the "Administrators" group

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **System** > **Security** > **2-step Verification**.
   QTS displays a list of users and their 2-step verification status.

   Tip

   You can select an option from the drop-down list to view the current status of local users, local groups, domain users, and domain groups.

Status	Description
Enabled	2-step verification is enabled for this user.
Disabled	2-step verification is disabled for this user.
Incomplete	2-step verification is enforced for this user, but this user has not completed the setup.

3. Select users or groups on whom you want to enforce 2-step verification.
4. Click **Apply**.
   The verification status of the selected users changes from `Disabled` to `Incomplete`. When the selected users complete the setup, the status will change to `Enabled`.

Disabling 2-step verification

After disabling 2-step verification, you will only be able to verify your identity with your password. Disabling 2-step verification makes your account less secure. If possible, QNAP recommends using 2-step verification to enhance your account and device security.

Important

This topic explains how to disable 2-step verification for your own account. If you are an administrator and want to disable 2-step verification for other user accounts, go to **Control Panel** > **Privilege** > **Users** and then edit their account profile settings.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **2-Step Verification** tab.
4. Under **Protect your account with 2-Step Verification**, click **Disable**.
   The **Verify Your Identity** window appears.
5. Enter your password.
6. Click **OK**.

Passwordless login

Overview

Passwordless login simplifies and secures your login process by verifying your identity with your mobile device. To use passwordless login, you must install QNAP Authenticator.

Important

- You need the myQNAPcloud service and a QNAP ID to access the NAS via the Internet. You should set up myQNAPcloud and create your QNAP ID before enabling passwordless login.
- You cannot enable 2-step verification and passwordless login at the same time.

Supported Verification Methods

QTS supports the following verification methods for passwordless login. You can enable multiple verification methods, and you can choose freely from these methods upon each login.

Verification Method	Description
QR Code	Use QNAP Authenticator to scan a QR code displayed on the NAS login screen.
Login Approval	Approve a login request displayed on QNAP Authenticator.

Enabling passwordless login with a QR code

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Passwordless Login** tab.
4. Specify a recovery email address.

   Tip
   This allows the system to send messages to your email if you cannot access your mobile device. You can choose to use the personal email address specified in your user profile or another email as the recovery email address.
5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **QR Code**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.
11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and adds your NAS to the device list.
13. Click **Next**.
14. Optional: Enable the Login Approval method.
15. Click **Finish**.
    QTS displays a summary of your passwordless login settings.

Passwordless login is now enabled for your account. Starting from your next login, you can verify your identity with a QR code without entering your password.

Enabling passwordless login with a login approval

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Passwordless Login** tab.
4. Specify a recovery email address.

   Tip
   This allows the system to send messages to your email if you cannot access your mobile device. You can choose to use the personal email address specified in your user profile or another email as the recovery email address.
5. Click **Get Started**.
   The **Verify Your Identity** window appears.
6. Enter your password to confirm this action.
7. Click **OK**.
   QTS displays available verification methods in a new window.
8. Select **Login Approval**.
9. Click **Start**.
10. On your mobile device, download and install QNAP Authenticator from Apple App Store or Google Play.
11. Click **Next**.
12. Open QNAP Authenticator and scan the QR code displayed on the computer screen.
    QNAP Authenticator connects to your NAS and displays a verification code.
13. Verify whether QTS displays the same verification code.
14. On your QNAP Authenticator, tap **Approve** if both verification codes match.
    The **Verify Your Identify** window appears on the NAS.
15. Enter your password.
16. Click **OK**.
17. Optional: Enable the QR Code method.
18. Click **Finish**.
    QTS displays a summary of your passwordless login settings.

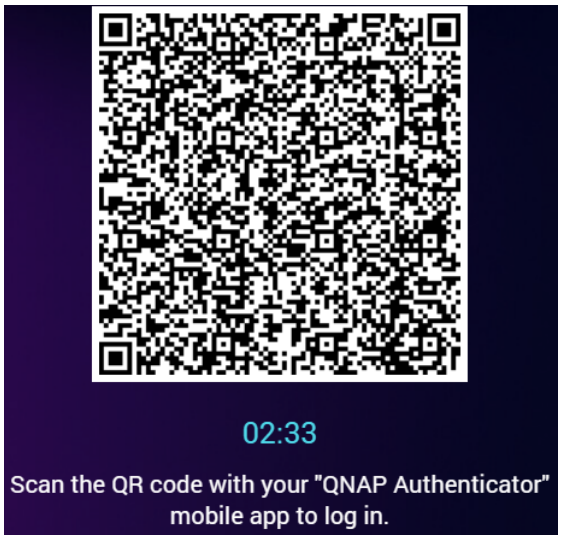
Passwordless login is now enabled for your account. Starting from your next login, you can verify your identity with a login approval without entering your password.

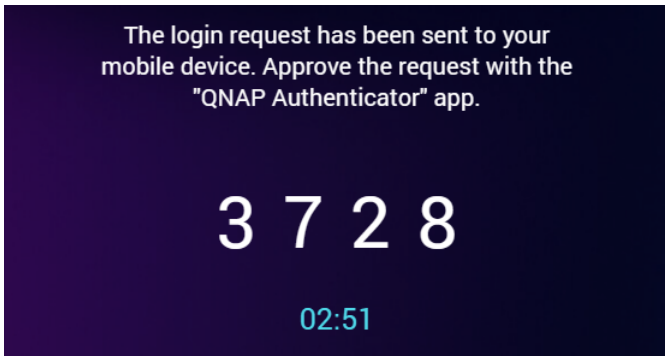
Logging in without your password

When Passwordless Login is enabled, you can verify your identity using QNAP Authenticator on your mobile device, or through a verification code sent to your email if your mobile device is not available.

1. Connect to your NAS.
   The system displays the login screen.
2. Enter your username.
3. Click **Next**.
4. Verify your identify.

> **Tip**
> You can click **Try another way** to select a different verification method.

Verification Method	User Action
QR Code	Open QNAP Authenticator and scan the QR code displayed on the NAS login screen. 

Verification Method	User Action
Login Approval	**a.** Verify whether the NAS and QNAP Authenticator display the same security code.  **b.** Tap **Approve** on QNAP Authenticator.
Email	**a.** Enter the verification code sent to your email address. **b.** Click **Next**.

Tip
You can still access the NAS using your password by clicking **Enter your password**.

After scanning the QR code or approving the login request, you are logged in to the NAS. The system displays the desktop and is ready for use.

Tip
If you cannot access the NAS with these methods due to the unavailability of your mobile device and your own password, you can press the reset button on the NAS for 3 seconds to activate the default administrator account "admin", restore its default password (the Cloud Key of the device), and then log in to the NAS with this "admin" account. You can then reset the password of your own account. Nevertheless, after completing the setup, you should disable the "admin" account to ensure system security.

Disabling passwordless login

After disabling passwordless login, you will only be able to verify your identity with your password.

1. Click your username on the desktop task bar.
2. Select **Login and Security**.
   The **Login and Security** window appears.
3. Go to the **Passwordless Login** tab.

4. Under **Protect your account with Passwordless Login**, click **Disable**.
   The **Verify Your Identity** window appears.
5. Enter your password.
6. Click **OK**.

Passwordless login is disabled. You can only verify your identity with your password.

Support and other resources

QNAP provides the following resources:

Resource	URL
Documentation	https://download.qnap.com
Compatibility List	https://www.qnap.com/compatibility
NAS Migration Compatibility	https://www.qnap.com/go/nas-migration
Expansion Unit Compatibility	https://www.qnap.com/go/compatibility-expansion
Service Portal	https://service.qnap.com
Product Support Status	https://www.qnap.com/go/product/eol.php
Downloads	https://download.qnap.com
Community Forum	https://forum.qnap.com
QNAP Accessories Store	https://shop.qnap.com

2. Getting Started

After completing hardware setup and firmware installation, you can start creating storage pools and volumes to store your data and then configure user accounts to control access to your data. To access and manage your files via the internet, you can set up remote access and enable the myQNAPcloud service for your device. To ensure data availability, you can back up your NAS data to multiple destinations using various backup solutions.

In addition to built-in features, you can also install applications and purchase software licenses to add functionality to your device. To protect your data from security threats, you should take action to prevent unauthorized access, update your software regularly, and use security utilities to secure your QNAP device.

Storing data

To store data on the NAS, you must create storage pools, volumes, and shared folders, which are features designed to help you facilitate data storage and management. You can configure storage settings in Storage & Snapshots, a powerful built-in utility for storage and snapshot management in QTS.

1. Create a storage pool.
   A storage pool combines multiple physical disks into one large storage space and may contain one or more RAID groups. You need to create at least one storage pool. You can also choose a RAID type that meets your needs for data redundancy and storage performance.
   For details, see Creating a storage pool.

2. Create a volume.
   A volume is a storage space created from a storage pool or a RAID group, allowing you to divide and manage available storage capacity. QTS provides several volume types for different combinations of performance and flexibility. You need to create at least one volume to start storing data on the NAS.
   For details, see Volume creation.

3. Create a shared folder.
   A shared folder is created on a volume, allowing you to access, manage, and share your files. QTS automatically creates several default shared folders for various purposes. You can create more shared folders and configure their access permission settings to better manage your files.
   For details, see Creating a shared folder.

Accessing data

QTS provides several simple ways to access your data on the NAS when your NAS and computer are on the same local network. With a web browser, you can access and manage your files using File Station in QTS. You can also access mounted shared folders directly via the file manager on your Windows or macOS computer.

- Access files via File Station.

  a. Access the NAS.
  You can directly access the NAS via its IP address using a web browser. You can also discover and access your NAS on the local network using Qfinder Pro.
  For details, see:

  - Accessing the NAS using a browser
  - Accessing the NAS using Qfinder Pro

  b. Open File Station.
  File Station is the file manager in QTS, allowing you to browse, manage, and share files on the NAS. You can also create and configure shared folders in File Station to facilitate file management.
  For details, see File Station.

- Access files via shared folders mounted on your computer.
  You can mount a shared folder as a network drive on your computer. This allows you to directly access mounted shared folders using the file manager on your Windows or macOS computer.
  For details, see:

  - Mapping a shared folder on a Windows computer
  - Mounting a shared folder on a Mac computer

Backing up data

Regular backup is crucial for data protection. QNAP provides various backup solutions to ensure the availability of your data. You can start backup up your files with the following tools designed to meet your essential backup needs.

Hybrid Backup Sync allows you to back up, restore, and synchronize the data on your local NAS to remote NAS, external devices, cloud storage services, and vice versa. You can also take snapshots for the volumes on your local NAS and then use Snapshot Replica to back up these snapshots to a remote NAS.

- Use Hybrid Backup Sync to back up your NAS data.

  a. Install Hybrid Backup Sync on the NAS.

  b. Create a backup job or a sync job.

  Hybrid Backup Sync is a comprehensive solution for data backup and disaster recovery. You can create several types of backup and sync jobs between the local NAS and multiple destinations (including remote NAS, external devices, and cloud storage services). Hybrid Backup Sync enhances data deduplication and encryption for your backup data. This essential tool also provides various features to facilitate job configuration and management.

For details, see Hybrid Backup Sync Help.

- Take and back up snapshots for your NAS data.

  a. Take snapshots for volumes.

  b. Use Snapshot Replica to back up snapshots.

  An essential feature for data protection, a snapshot records the state of a volume at a specific point in time. Using a snapshot, you can restore a volume to a previous state or restore the previous versions of files or folders. You can view and manage your snapshots in Storage & Snapshots.
  To further protect your data, you can use Snapshot Replica to back up your snapshots to another storage pool on the local NAS or to a remote NAS. In the event of a disaster, you can choose to recover your data on the source NAS or on the destination NAS.
  For details, see:

  - Taking a snapshot
  - Creating a Snapshot Replica job

Configuring privilege settings

QTS allows you to create user accounts and user groups, specify user privileges, and configure shared folder permissions. These features are essential for data security and management.

The admin account is the default administrator account in QTS. To enhance your data and device security, we recommend creating another administrator account and then disabling the admin account.

1. Create an administrator account.
   You can create a new user account to replace the admin account. To grant administrator privileges to this new user, you must add this new user to the administrator group. You should also grant shared folder access permissions to this user.
   For details, see Creating an administrator account.

2. Disable the admin account.
   After creating a new administrator, you should disable the default admin account and then start managing the NAS with this new administrator account.
   For details, see Disabling a default administrator account.

3. Create more users or user groups.
   You can create other users or user groups and grant them different levels of privileges to control access to your data on the NAS.
   For details, see:

   - Creating a local user
   - Creating a user group

Setting up remote access

myQNAPcloud is a QNAP service that allows you to connect to the NAS via the internet. With this service, you can remotely access your data on the NAS and use a wide variety of mobile applications designed for the QNAP NAS wherever you go. To use the myQNAPcloud service, you must first create a QNAP ID and then register your NAS to your QNAP ID.

1. Create a QNAP ID.
   QNAP ID is your QNAP account that allows you to access various QNAP services. To create a QNAP ID, go to https://account.qnap.com.
   For details, see Creating a QNAP ID.

2. Set up myQNAPcloud on your device.
   After creating a QNAP ID, you need to enable the myQNAPcloud service on your NAS and then associate your device with your QNAP ID. You can also configure various remote access settings in myQNAPcloud.
   For details, see myQNAPcloud.

3. Remotely access the NAS via myQNAPcloud.
   After setting up myQNAPcloud on your NAS, you can remotely access and manage the NAS via the myQNAPcloud website or via the SmartURL generated for your NAS.

4. Remotely access the NAS on your mobile device.
   QNAP provides a wide range of mobile applications that enable you to access, manage, monitor, and back up your NAS wherever you go. After installing these QNAP applications on your mobile devices, you must sign in to them with your QNAP ID.
   For details, go to https://www.qnap.com/go/mobile-apps.

Acquiring apps and licenses

QTS provides various essential applications to help manage your NAS. In addition to these built-in features, QTS also allows you to install more applications from the App Center to further enhance the functionality of your device. To gain access to certain advanced features and premium products, you must purchase and activate licenses for your device.

1. Install applications in the App Center.
   App Center provides a wide variety of applications and utilities. You can also manage and update your installed applications in the App Center.
   For details, see App Center.

2. Purchase licenses in the QNAP Software Store.
   QNAP Software Store is an online store where you can purchase licenses and manage your orders. QNAP provides various types of licenses and subscription plans to meet different needs and usage environments.
   For details, see Licenses.

3. Activate licenses in the License Center or License Manager.
   Some licenses are automatically activated after being purchased. However, sometimes you must manually activate a license.
   License Center allows you to manage licenses on your local device. License Manager allows you and your organization to manage licenses under your QNAP ID.

For details, see Licenses.

Securing the NAS

All networked devices face constant security threats. To reduce the risk of your data being attacked, we strongly recommend following the best practices to secure your NAS. In essence, you should prevent unauthorized access, update your device software regularly, and install security utilities to protect your device.

1. Prevent unauthorized access to your device.

   a. Create a new administrator account and disable the admin account.
   The admin account is the default administrator account. Nevertheless, to enhance the security of your device, we strongly recommend creating another administrator account and then disabling the admin account.
   For details, see Default administrator account.

   b. Enhance user password strength.
   We recommend enhancing your password strength and changing your passwords regularly to prevent brute-force attacks.
   For details, see Modifying user account information.

   c. Set up 2-step verification.
   2-step verification further enhances the security of user accounts by requiring users to specify a security code in addition to their account credentials during the login process.
   For details, see 2-step verification.

   d. Remove unknown or suspicious accounts.
   We recommend verifying user accounts regularly and deleting any unknown or suspicious accounts.
   For details, see Deleting users.

   e. Remove unnecessary permissions from general users.
   We recommend restricting the permissions of non-administrator users to limit their access to system operations and sensitive data. This helps mitigate the impact of a compromised user account.
   For details, see Modifying user account information.

   f. Remove unknown or suspicious applications.
   We recommend only installing applications and utilities that have digital signatures, which validate software developed by QNAP and other QNAP-trusted developers.
   You should regularly check your installed applications and remove any unknown or suspicious applications from the App Center.
   For details, see Digital signatures and Uninstalling an app.

   g. Configure access settings in myQNAPcloud.
   To ensure your data security, UPnP is disabled by default. We recommend manually configuring port forwarding settings on your router.
   We also recommend configuring access control and only publishing necessary services in myQNAPcloud.
   For details, see:

      - Configuring UPnP port forwarding

- Configuring device access controls for stand-alone devices

2. Update your firmware and applications to the latest versions.

   a. Update the firmware to the latest version.
   We strongly recommend regularly updating the firmware of your device to the latest version to benefit from the latest features, enhancements, and security fixes. You can also choose to automatically check for and install available updates.
   For details, see Firmware update.

   b. Update applications to the latest versions.
   You should regularly update your installed applications to their latest versions for better performance, functionality, and security. App Center allows you to check for all available updates and then install updates for multiple applications at the same time.
   For details, see:

   - Updating an app
   - Batch updating multiple apps

3. Install and run security utilities on the NAS.

   a. Run Malware Remover.
   Malware Remover is a built-in utility designed to protect QNAP devices against malicious software. You can run instant or scheduled scans to remove malicious software from your device.
   For details, see Malware Remover.

   b. Install and run Security Counselor.
   Security Counselor is the security portal that allows you to centrally configure security settings and manage security components on your QNAP device. You can choose security policies, scan the device, and check for potential security weaknesses on the device. Security Counselor identifies potential risks and provides suggestions to help you enhance device security. You can also subscribe to QNAP security advisories to stay informed of the latest security fixes and solutions.

3. 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.
Console Management	This screen allows you to enable console management.

Configuring system administration settings

1. Go to **Control Panel** > **System** > **General Settings** > **System Administration**.
2. Specify the following information.
   a. **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
      - Dashes (-)

Important

- The server name must contain one or more letters.
- The server name cannot consist of numbers only.
- The server name cannot start with a dash.
- The host name must contain one or more letters.
- The host name cannot consist of numbers only.
- The host name cannot start with a dash.

b. **System port**: Specify the port used to access the web interface.

Tip
The default port is 8080.

c. **Enable HTTP compression**: Select this option to improve transfer speeds and bandwidth utilization. This setting is enabled by default.

Warning
Enabling this option may lead to security risks.

d. **Enable secure connection (HTTPS)**: Select this option to allow HTTPS connections.

1. Select **Enable secure connection (HTTPS)**.
2. Select a TLS version.
   The default TLS version is 1.2.

   Warning
   Selecting the latest TLS version may decrease compatibility for other clients in your system.
3. Enable strong cipher suites.
4. Specify a port number.
5. Optional:
   Select **Force secure connection (HTTPS) only** to require all users to connect to the NAS using only HTTPS.

e. **Custom "Server" HTTP header**: Select this option to specify a server HTTP header.

f. **Do not allow QTS embedding in IFrames**: Select this option to prevent websites from embedding QTS using IFrames.

1. Click **Allowed Websites** to allow a specific website to embed QTS in IFrames.
2. The **Allowed Websites** window appears.

3. Optional:
   Click **Add** to add a website to the list.
   The **Add Host Name** window appears.
4. Specify a host name.
5. Click **Add**.
   The host name is added to the allowed websites list.
6. Optional:
   Select a website, and then click **Delete** to delete a website from the list.
7. Click **Apply**.

g. **Enable X-Content-Type-Options HTTP header**: Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities.

h. **Enable Content-Security-Policy-HTTP header**: Select this option to protect your device from attacks that exploit Cross Site Scripting (XSS) and data injection vulnerabilities.

i. **Redirect URL to NAS login page**: Select this option to enable redirecting the URL to the NAS login page.

Important

- QNAP recommends disabling this feature to prevent your NAS system from being exposed to the public.
- If you have disabled the **Web Server** and entered the NAS IP address without the system port, the URL will be redirected to the NAS login page.
- You can check the web server settings by going to **Control Panel** > **Applications** > **Web Server**.

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.
Synchronize with a 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 • Optional: Click **Test Connection**. The system will test if a connection can be established with the configured time server. • **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**.

Action	Steps
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 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**.

Enabling or disabling console management

Console Management is a text-based tool that helps the admin account perform basic configuration or maintenance tasks.

1. Go to **Control Panel** > **System** > **General Settings** > **Console Management**.
2. Optional: Select **Enable Console Management**.

> **Note**
> **Enable Console Management** is enabled by default.

3. Deselect **Enable Console Management** to disable the feature.
4. Click **Apply**.

Security

To protect your NAS from unauthorized access, you can configure allow or deny lists, enable IP access protection, upload SSL certificates and custom root certificates. Additionally, you can use account access protection or create a unique password policy for your NAS.

Configuring the allow/deny list

Important
If you have installed QuFirewall on your device, go to QuFirewall to configure the allow or 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 in the IP deny list. **Tip** To remove an IP address, netmask, or IP range, select an entry from the table, and then click **Remove**.	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**.
Use IP allow list	The NAS can only connect to the IP addresses or network domains included in the IP allow list. **Tip** To remove an IP address, netmask, or IP range, select an entry from the table, and then click **Remove**.	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**.

3. Click **Apply**.

Configuring IP access protection

You can configure your NAS to automatically block client IP addresses after too many failed login attempts within a specified time period.

1. Go to **Control Panel** > **System** > **Security** > **IP Access Protection**.

2. Select the connection methods you want to protect.

   Note
   SSH, **Telnet**, and **HTTP(S)** are enabled by default.

3. Optional: Specify the following information:

Field	Description
Time interval	The interval of time in which the system counts successive failed login attempts.
Failed login attempts	The number of failed login attempts allowed within the specified time interval.
IP block length	The amount of time the IP address is blocked.

   Note
   - A time interval of 0 means the IP address will be blocked if the specified number of failed login attempts is reached, regardless of when those login attempts occurred.
   - For example, if **Time interval** is set to 5 and **Failed login attempts** is set to 3, then the IP address will be blocked if the user attempts to login 5 times within 3 seconds.

4. Click **Apply**.
   If the time interval for any connection method is set to 0, you must verify your account password to apply the changes.

Configuring account access protection

1. Go to **Control Panel** > **System** > **Security** > **Account Access Protection**.
2. Specify the user type.
3. Select the connection methods you want to protect.
4. Optional: Specify the following information.
   - Time period
   - Maximum number of unsuccessful login attempts within the time period
5. Click **Apply**.

SSL 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 a Secure Sockets Layer (SSL) certificate from a trusted provider through Server

Certificate or import a custom root certificate to your QNAP device. QNAP recommends you purchase a valid SSL certificate from myQNAPcloud SSL Web Service Certificate. For details, see myQNAPcloud website.

Replacing the server certificate

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.

1. Go to **Control Panel** > **System** > **Security** > **SSL Certificate & Private Key**.
2. Go to **Server Certificate**.
3. Click **Replace Certificate**.
   The **Replace Certificate** window appears.
4. 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. **Note** QNAP recommends you use port 80 or 443 for authorizing the SSL certificate domain and accessing the Internet.
Create self-signed certificate	This option allows you to create a self-signed certificate.

5. Click **Next**.
   A configuration window appears.

6. Perform any of the following actions:

Option	User Action
Import certificate	**a.** Click **Browse** to upload a valid certificate. **b.** Click **Browse** to upload a valid private key. **c.** 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`
Create self-signed certificate	Configure the following information: **Private key length**, **Common name**, **Email**, **Country**, **State/Province/Region**, **City**, **Organization**, **Department**.

7. Click **Apply**.

Downloading the server certificate

1. Go to **Control Panel** > **System** > **Security** > **SSL 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.

Managing a root certificate

1. Go to **Control Panel** > **System** > **Security** > **SSL Certificate & Private Key**.
2. Go to **Custom Root Certificate**.

3. Select one of the following actions:

Action	
Import a root certificate	**a.** Click **Import**. The **Import Certificate** window appears. **b.** Click **Browse**. The file upload window appears. **c.** Select a file. **Important** The root certificate file cannot be larger than 1 MB. The following file formats are supported: *.PFX, *.P12, *.PEM, *.crt, *.cert **d.** Click **Next**. The certificate description page appears. **e.** Click **Import**. The imported root certificate is displayed in the client certificate table.
Edit a root certificate	**a.** Click  . The **Edit Root Certificate** window appears. **b.** Edit the certificate description. **c.** Click **Apply**.
Delete a root certificate	**a.** Select a root certificate. **b.** Click **Delete**. A confirmation message appears. **c.** Click **Yes**.

Configuring the password policy

Important

The following password policy is configured by default:

- English letters: No restrictions
- Digits: Enabled
- Minimum length: 8

1. Go to **Control Panel** > **System** > **Security** > **Password Policy**.

2. Optional: Under **Password Strength**, configure any of the following password criteria.

Criteria	Description
English letters	Passwords must contain at least one letter. Select **At least 1 uppercase and 1 lowercase** to require at least one uppercase and one lowercase letter.
Digits	Passwords must contain at least one number.
Special characters	Passwords must contain at least one special character.
Must not include characters repeated three or more times consecutively	Repeating characters are not allowed. For example, `AAA`.
Must not be the same as the associated username, or the username reversed.	The password must not be the same as the username or the reversed username. For example, username: `user1` and password: `1resu`.
Minimum length	The password length must be greater than or equal to the specified number. Specify a value between 4 and 64 characters.

3. Optional: Require users to periodically change their passwords.

Important
Enabling this option disables **Disallow the user to change password** under user account settings.

   a. Select **Require users to change passwords periodically**.
   b. Specify the maximum number of days that each user password is valid.
   c. Optional: Select **Send a notification email to users a week in advance before their password expires**.

4. Click **Apply**.

Hardware

You can configure general hardware settings, audio alerts, smart fan settings, and view all Single Root I/O Virtualization (SR-IOV) settings.

Note
SR-IOV settings only appears if the hardware supports it.

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, 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. **Important** Some QNAP NAS models that use NVMe solid-state drives do not support disk 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.
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 redundant power supply mode	Select this option to enable alerts and notifications in case of redundant PSU failures. With this option enabled, a redundant PSU failure will trigger the following: • A desktop notification • An audio alert • The system status LED becomes red
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.
Do not shut down using the power button	Select this option to disable the power button. When this option is enabled, pressing the power button will not shut down the device. **Note** This feature is only available on certain models.
Enable disk auto recovery	Select this option to allow the system to automatically reconnect any disks that have been unintentionally disconnected from the system. Enabling this feature helps speed up the RAID group rebuild process and enhance overall storage stability, but might have a slight impact on write performance. **Note** This feature is only available on certain 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 to trigger an audio alert every time the NAS starts, shuts down, or upgrades firmware.
System events	Select to trigger an audio alert when errors or warnings occur.

Setting	Description
Enable speech notification	Select 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
Automatically adjust fan speed (recommended)	Select from the two automatic fan speed adjustment options. **a.** QTS monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. **b.** 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.
Manually set fan speed	Move the slider to set the fan speed.

3. Click **Apply**.

Configuring hardware resource settings

You can configure and allocate expansion card resources for different software QTS applications in Hardware Resource Settings. You can also configure Thunderbolt expansion cards, AI accelerators, or network expansion cards that support SR-IOV.

For details, see Viewing Single Root I/O Virtualization (SR-IOV) settings

1. Go to **Control Panel** > **System** > **Hardware** > **Hardware Resources**.
   QTS lists the available expansion cards.
2. Identify the expansion cards you want to configure.
3. Under **Resource Use**, select an OS or an application.

   Note
   Some functions are only applicable for certain models and expansion cards.

OS or Application	Description
QTS	QTS applications share expansion card resources for transcoding. • Select **Hardware Transcoding** to allow QTS software to use expansion card resources to speed up transcoding tasks. Only one card can be assigned to hardware transcoding. • Select **Output** to use expansion 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 expansion card resources.
Container Station	Container Station has exclusive use of all expansion card resources.

4. Click **Apply**.

Configuring Hailo-8 settings

You can configure the priority level and maximum number of Hailo-8 devices allocated to an app.

Important

- The system will not run apps with lower priority levels until Hailo-8 devices are released from running higher priority apps.
- You can allocate up to four Hailo-8 devices to an app.

1. Go to **Control Panel** > **System** > **Hardware** > **Hardware Resource**.
2. Locate and click a Hailo-8 device from the list.
   The **Halio-8 Priority Settings** window appears.
3. Select an app.
4. Select a Hailo-8 priority level.
5. Select the maximum number of Hailo-8 devices.
6. Click **Apply**.

Configuring TPU settings

You can configure the priority level and maximum number of Tensor Processing Units (TPU) allocated to an app.

Important

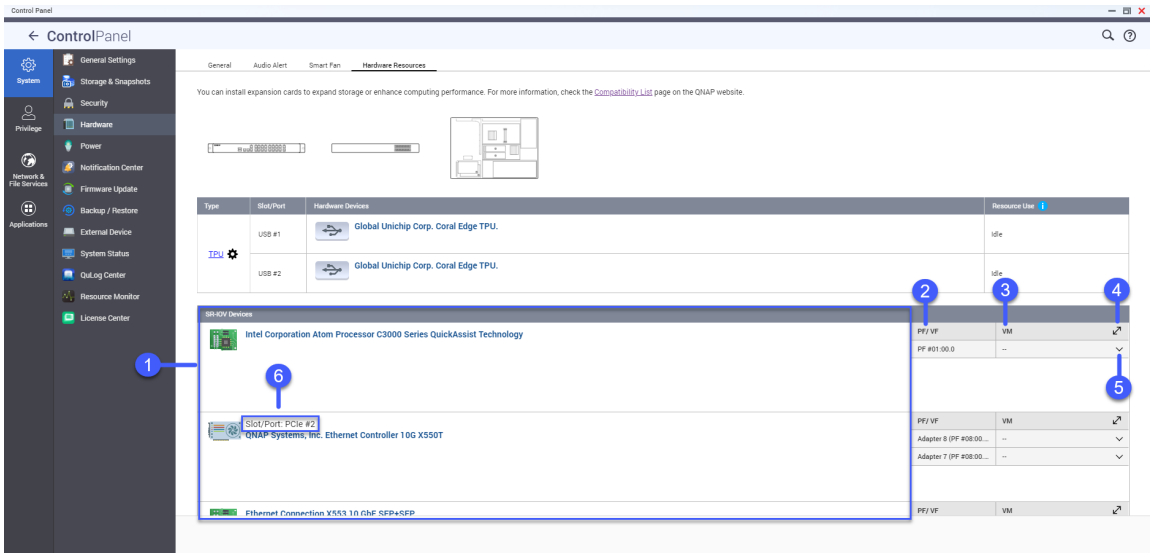
- The system will not run apps with lower TPU priority levels until the TPU resource is released from running higher priority apps.
- You can allocate up to four TPU devices to an app.

1. Go to **Control Panel** > **System** > **Hardware** > **Hardware Resource**.
2. Locate and click a TPU device from the list.
   The **Priority** window appears.
3. Select an app.
4. Select a TPU priority level.
5. Select the maximum number of TPUs.
6. Click **Apply**.

Viewing Single Root I/O Virtualization (SR-IOV) settings

You can view all Single Root I/O Virtualization (SR-IOV) devices mapped to your virtual machines on the **Control Panel** > **Hardware** > **Hardware Resources** page. The SR-IOV interface is a hardware specification that allows a single PCIe device, such as a network adapter, to appear as multiple physical devices to the hypervisor. Because each device is directly assigned to an instance, it can bypass the hypervisor and virtual switch layer to achieve low latency and performance matching in nonvirtualized environments. SR-IOV achieves this through the following types of functions:

- Physical Function (PF): These are PCIe devices that have SR-IOV capabilities. PFs are managed and configured in the same way as PCIe devices.
- Virtual Function (VF): These are lightweight PCIe functions that only process I/O. Because each VF is derived from a PF, the device hardware limits the number of VFs a device can have. A VF shares one or more hardware resources of the device, such as a memory or network port.
  The following table lists all SR-IOV functions you can view in **Hardware Resource**:



No.	Settings	Description
1	SR-IOV Devices	Lists all the SR-IOV devices that are mapped to your virtual machine (VM).
2	PF/VF	Displays the physical function (PF) or virtual function (VF) configured to the SR-IOV device.
3	VM	Shows the virtual machines that are mapped to the PF or VF.
4	Resize	Click to enlarge or minimize the SR-IOV device panel window.
5	Show or Hide	Click to show or hide the list of SR-IOV device details.
6	Slot/Port	Shows the slot/port type and slot/port number.

For details on how to configure an SR-IOV device to a VM, see the Virtualization Station user guide.

Power

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

Configuring EuP mode

Energy-using Products (EuP) is a regulatory directive designed to improve the energy efficiency of electrical devices, reduce the use of hazardous substances, and to reduce the environmental impact of the product. To comply with the EuP directive, EuP mode can be enabled on your QNAP NAS.

1. Go to **Control Panel** > **System** > **Power** > **EuP Mode Configuration**.

2. 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.

3. Click **Apply**.

Enabling or disabling Wake-on-LAN (WOL)

You can power on the NAS remotely using the Wake-on-LAN (WOL) protocol in Qfinder Pro. 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.

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

Configuring the power recovery settings

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

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**.

Configuring the Power Schedule

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

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. • **Power action**: Select whether you want to shut down, restart, or turn on the NAS. • **Schedule**: Select the frequency of the action. • **Start time**: Select the time of day to perform the action.
Remove a scheduled action	**a.** Select one or multiple schedules. **b.** Click **Remove**.
Edit scheduled action	**a.** Select one a schedule. **b.** Click  in the action column. The **Edit Power Schedule** window appears. **c.** Edit the power schedule. **d.** Click **Apply**.
Enabled/disable a scheduled action	**a.** Select one a schedule. **b.** Click  in the action column. The **Edit Power Schedule** window appears. **c.** Select or deselect **Enable schedule**. **d.** Click **Apply**.

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

External device

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.

Phase	Scenario	NAS Behavior
Phase 3: From the moment the UPS runs out power until the power is restored	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.

UPS events and corresponding NAS behavior

The Uninterruptible Power Supply (UPS) events handled by the NAS during power disruptions include OnLine (OL), OnBattery (OB), OnSmartBoost (OSB), OFF (OFF), and OnBatteryTest (OBT). The NAS performs auto-protection or shutdown mode depending on the detected UPS status and your configured power failure settings. The following table describes the events and the corresponding NAS behavior.

UPS Event	Definition	NAS Status	NAS Action
OnLine (OL)	The UPS is operating normally.	Normal	None
OnSmartBoost (OSB)	The UPS is operating on smart boost mode.	Normal	None
OnBatteryTest (OBT)	The UPS is in battery test mode.	Normal	None
OnBattery (OB)	The UPS is operating on the backup battery.	Abnormal	The NAS enters auto-protection or shuts down.
OFF (OFF)	The UPS is not operating.	Abnormal	The NAS powers off.

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	User Actions
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.** Configure the SNMP community. **e.** 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

Mode	User Actions
Network standby UPS	**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**.

Configuring USB settings

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

Setting	Options
Disallow USB Devices	**a.** Select **Disallow USB Devices**. **b.** Choose one of the following options. • Disallow all USB device types **Note** All USB device types include: UPS, WiFi dongles, USB cameras, USB mouses, USB keyboards, USB speakers; and external USB storage devices such as USB flash drives, external hard drives, QNAP JBOD storage enclosures, and QNAP RAID expansion enclosures. This will also disable USB One Touch Copy and disallow file transfers from mobile devices. • Disallow only USB storage devices **Note** USB storage device types include: external USB storage devices such as USB flash drives, external hard drives, QNAP JBOD storage enclosures, and QNAP RAID expansion enclosures. This will also disable USB One Touch Copy and disallow file transfers from mobile devices.

3. Click **Apply**.
4. Click **Restart Now** to restart the NAS.

Firmware update

> **Important**
> On devices with QTS 4.5.4 or earlier, if the SQL server is enabled during the firmware update, the system automatically downloads the MariaDB 5 app and migrates the SQL server data to MariaDB.
> For details, see Configuring the MariaDB database.

QNAP recommends keeping your NAS firmware up to date. This ensures that your NAS benefits from new software features, security updates, enhancements, and bug fixes. By default, QTS automatically checks for firmware updates on a daily basis.

You can update the NAS firmware using one of the following methods:

Update Method	Description
Using **Check for Updates**	The system will check for the available updates. If updates are available, they can be downloaded and installed immediately or postponed to a later date. For details, see Checking for updates.
Using automatic updates	You can configure QTS to periodically download and install the latest firmware updates. For details, see Updating the firmware automatically.
Using **Manual Installation**	You can check for firmware updates on the QNAP website, download updates to a computer, and manually install updates onto your device. For details, see Updating the Firmware Manually.
Using **Qfinder Pro**	If your device is connected to the local area network, you can use Qfinder Pro to check and install the latest firmware updates. For details, see Updating the firmware using Qfinder Pro.

The following types of firmware updates are available:

Update Type	Description
Critical update	Critical updates provide fixes for critical security vulnerabilities and critical system issues. These updates are appropriate for users who have high security demands.

Update Type	Description
Quality update	Quality updates provide bug and security fixes, and fixes for critical system issues. These updates are appropriate for users who have high system reliability demands.
Latest update	The latest updates provide new features, enhancements, bug fixes, and security updates. These updates are appropriate for users who want to try the newest features and enhancements.
Beta update	These updates provide access to the latest features that have not been officially released. Given that beta features are still under testing, these updates may not be as stable as official releases.

Firmware update requirements

Your device must meet the following requirements to perform a firmware update:

Settings	Requirements
Hardware settings	• A computer **Important** A computer is required when updating the firmware using **Manual Installation** or Qfinder Pro. • Ethernet cables **Important** QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection remains stable during the firmware update process.
System reboot	QNAP recommends rebooting the NAS system before the firmware update.
Administrator privileges	You must be a NAS administrator or have admin privileges to update firmware.
Stop NAS operations	QNAP recommends stopping all other NAS operations before the firmware update. The NAS must restart before the firmware update takes effect and this may disrupt ongoing NAS services or operations.

Settings	Requirements
Device model name	Ensure you have the correct NAS model name. You can find the NAS model name using the following methods: • Locate the model name on a sticker on the bottom or rear of your device. • Go to **Control Panel** > **System Status** > **System Information** > **Model name**
Firmware version	If you are updating the firmware using **Manual Installation** or Qfinder Pro, ensure the selected firmware version is correct for your device model.

Checking for updates

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details about data backup, see System backup and restore.
- Do not power off your device during the firmware update process.

Important

- Read the Firmware update requirements before updating the firmware.
- The update may require several minutes or longer depending on your hardware configuration and network connection.

1. Go to **Control Panel** > **System** > **Firmware Update** > **Firmware Update**.
2. Click **Check for Updates**.
   - QTS checks for available firmware updates. You can choose to update QTS if an update is available.
   - If the system has been running for longer than seven days, QNAP recommends restarting the device before updating the firmware. For details, see Firmware update requirements.
3. Select the firmware update to download and install.

   Note
   For information on the types of available firmware updates, see , see Firmware update.
4. Optional: Click **Release notes** to view the release notes of the firmware update.
5. Optional: Select **Automatically restart the system if required for this update**.

6. Click **Update**.
   If the system has been running for longer than seven days, a confirmation window appears. QNAP recommends restarting the device before you proceed. Otherwise, the selected firmware update is downloaded and installed.
7. Optional: In the confirmation window, click **Restart NAS**.
   The device immediately restarts. After the device restarts, repeat these steps from the beginning.

Updating the firmware automatically

Enabling automatic updates ensures the operating system is up to date by automatically downloading and installing firmware updates at regular intervals of time. You can also configure automatic notifications for available firmware updates.

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details about data backup, see Backup/Restore.
- Do not power off your device during the firmware update process.

Important

- Read the Firmware update requirements before updating the firmware.
- The update may require several minutes or longer depending on your hardware configuration and network connection.
- All ongoing tasks are suspended during the auto update. To prevent loss of data, the system cancels the update if there are any live iSCSI or Fibre Channel connections to the device, or virtual machines running in Virtualization Station.
- QNAP recommends checking for available updates by going to **Control Panel** > **System** > **Firmware Update** > **Firmware Update** > **Firmware Update Settings** and clicking on **Check for Updates** before enabling automatic firmware updates.

1. Go to **Control Panel** > **System** > **Firmware Update** > **Firmware Update** > **Firmware Update Settings**.

2. Select one of the following firmware update policies:

Update/Notification Behavior	Description & Action
Automatically install critical updates	• Critical firmware updates are downloaded and installed automatically within one hour of the time selected in **Update/Notification time**. • Notifications about upcoming automatic firmware updates are sent 12 hours before the update time.
Automatically install quality updates	• Quality firmware updates are downloaded and installed automatically within one hour of the time selected in **Update/Notification time**. • Notifications about upcoming automatic firmware updates are sent 12 hours before the update time.
Automatically install the latest updates	• The latest firmware updates are downloaded and installed automatically within one hour of the time selected in **Update/Notification time**. • Notifications about upcoming automatic firmware updates are sent 12 hours before the update time.
Notify me, do not automatically update	• Firmware updates are not automatically installed. • Notifications about available firmware updates are sent at the time specified in **Update/Notification time**. The system displays a notification window on the desktop when a new firmware update is available. You can choose to install, postpone, or skip an update.
Do not notify me, do not automatically update	• Firmware updates are not automatically installed. • Notifications about firmware updates are not sent.

3. If notifications or updates are enabled, then go to **Update/Notification time** and specify the time the update is downloaded and installed or notifications are sent.

Note

An automatic update starts within one hour from the scheduled time. You can cancel or postpone an automatic update. An update can be postponed up to 23 hours from the scheduled time that you originally specified.
If you select the policy **Notify me, but do not automatically update firmware**, the system will send update notifications at the specified time.

4. Optional: Select **Show desktop notifications for available firmware updates when an administrator logs in** to receive desktop notifications for available firmware updates when an administrator logs in.
5. Optional: Join the QNAP Beta Program.
   a. Select **Join the Beta Program and notify me when beta firmware updates are available**.
      The **QTS Beta Program** confirmation window opens.
   b. Select **I have read and agree to these terms**.
   c. Click **Yes, sign me up**.
      Desktop notifications of available beta firmware updates will appear when logging in.
6. Go to **Notification Rules** and create a notification rule for firmware updates. For details, see Creating an event notification rule.

   Tip
   To receive notifications for all firmware update activities, create notification rules that include all severity levels.
7. Click **Apply**.

The system saves the firmware update settings.

Updating the firmware manually

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details about data backup, see Backup/Restore.
- Do not power off your device during the firmware update process.

Important

- Make sure you read through the Firmware update requirements before updating the firmware.
- The update may require several minutes or longer, depending on your hardware configuration and network connection.

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.
   - Check for any additional firmware update setup instructions.

e. Ensure that the product model and firmware are correct.

f. Select the download server based on your location.

g. Download the firmware package.

h. Click **Browse**.

i. Select a folder.

j. Save the downloaded firmware package.

k. Extract the firmware package file.

2. Go to **Control Panel** > **System** > **Firmware Update** > **Manual Installation**.
3. Click **Browse** and then select the extracted firmware package file.
4. Click **Update System**.
   A confirmation message window appears.
5. Click **OK**.
   The device is immediately restarted.

Note
You can go to **Control Panel** > **QuLog Center** > **Local Device** > **Event Log** to check if the firmware installation was successful.

Updating the firmware using Qfinder Pro

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details about data backup, see Backup/Restore.
- Do not power off your device during the firmware update process.

Important

- Make sure you read through the Firmware Update Requirements 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 https://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.
      - Check for any additional firmware update setup instructions.
   e. Ensure that the product model and firmware version are correct.
   f. Download the firmware package.
   g. Extract the firmware package file.
2. Open Qfinder Pro.
   Qfinder Pro displays a list of NAS devices on your network.
3. Select a NAS model from the list.
4. Right click the device model on the list and then select **Update Firmware** .
   The **Firmware Update** window appears.
5. Specify your QTS username and password.
   Qfinder Pro displays the **Update Firmware** screen.
6. Select one of the following firmware update methods:

Methods	Steps
Update firmware manually	a. Click **Path of firmware package file**. b. Click **Browse**. c. Locate the downloaded firmware package file. d. Click **OK**.
Update firmware automatically	a. Click **Automatically update the firmware to the latest version**. b. Qfinder Pro searches for the latest firmware update.

7. Click **Start**.

System backup and restore

QTS provides system backup and restore features that allow you to perform the following actions:

- Back up and restore your system settings in the event of system failure

- Transfer your system settings to a new device
- Reset your system to factory default settings

Backing up system settings

In QTS, you can back up your system settings to a file known as a system configuration file. A system configuration file is a record of your system settings at a particular time. You can use a system configuration file to restore the system settings on your device to an earlier state, or transfer system settings to another device.

The following settings are recorded in each system configuration file:

- General system settings
- User and user group settings
- Shared folder settings
- Network settings
- Details of installed applications

You can configure an automatic backup schedule and also manually export the current system settings as a system configuration file and download the file to your computer at any time.

Note

To manually back up system settings on your QTS device, you must first configure an automatic backup schedule.

Important

The following cannot be backed up to, or restored from, a system configuration file:

- The power recovery setting (in **Control Panel** > **System** > **Power** > **Power Recovery**)
- Data in shared folders
- Specific application settings (including myQNAPcloud settings)

1. Go to **Control Panel** > **System** > **Backup / Restore** > **Backup/Restore Settings**.
2. Configure an automatic backup schedule.

Note

- The system can store a maximum of 10 backup system configuration files. If the maximum number is reached, each new backup replaces the oldest backup.
- The system will not create a new backup file if it detects no changes between the latest backup and the current system settings.

a. Under **Backup Schedule**, select **Enable backup schedule.**
The backup schedule settings appear.

b. Select a backup frequency.

c. Specify the backup time.

d. Select a destination folder on your device.

> **Note**
> Ensure the destination has at least 100 MB of free space for storing backup files.

e. Optional: Select **Encrypt the system configuration file**.
Specify a password and confirm the password.

f. Click **Apply**.
The system saves and enables the backup schedule.
The **Back Up Now** window opens.

g. Choose one of the following actions:

- **Back Up Now**: Back up the current system settings to a file in the specified destination folder.
- **Back Up Later**: Let the system back up system settings according to the configured schedule.

> **Tip**
> You can also click **Back Up Now** on the **Backup/Restore Settings** page at any time.

3. Download the current system settings to your computer.

a. Under **Download Current Settings**, click **Download to Computer**.
The **Back Up System Settings** window opens.

b. Review the backup information.

c. Optional: Select **Encrypt the system configuration file**.
Specify a password and confirm the password.

d. Click **Back Up**.
The system exports the current system settings as a system configuration file and downloads the file to your computer.

Restoring system settings

You can restore system settings on your QTS device from a system configuration file. The file can come from the same device or a different device, as long as the following requirements are met:

- The current device must run the same operating system as the one recorded in the system configuration file.

- The operating system version on the current device must be the same or a later version than the one recorded in the system configuration file.
- If you want to restore network settings, the current device cannot have fewer ports than the device recorded in the system configuration file.

QTS allows you to choose specific system settings to restore.

> **Note**
> For details on creating a system configuration file, see Backing up system settings.

1. Go to **Control Panel** > **System** > **Backup / Restore** > **Backup/Restore Settings**.
2. Under **Restore System Settings**, click **Restore**.
   The **Restore System Settings** wizard opens.
3. Import a system configuration file using one of the following methods:

Method	User Action
Upload file from computer	**a.** Click **Browse**. **b.** Locate a valid system configuration file on your computer. **c.** Upload the file.
Select file on current device	**a.** Click **Select Folder**. **b.** Locate the folder containing your system configuration files. **c.** Select a valid system configuration file.

4. Click **Next**.
   The **General** page appears.
5. Click **Next** to restore general system settings.
   To keep the existing general system settings on your device, click **Skip**.
   The **Users / Groups** page appears.
6. Configure the user and user group settings.
   To keep the existing users and user groups on your device, click **Skip** and go to the next step.

   > **Note**
   > Skipping restoring users and user groups also skips restoring shared folders.

   a. Optional: Select **Keep the current user account after restoration**.
      Specify a new password and then confirm the password.

Note

This option determines how your current user account is handled:

- If selected, your account will be restored from the configuration file and will be made an administrator. If your account is not in the configuration file, the system will use your current username to create a new administrator account. Selecting this option requires creating a new password.
- If deselected, only user accounts in the configuration file will be restored. Your current account will be deleted if it is not in the configuration file.

b. Click **Next**.

Warning

If the selected configuration file contains user or user group information that already exists on the current device, the information in the file will replace the information on the device.

The **Shared Folders** page appears.

7. Configure the shared folders to restore.
Skip this step if you skipped restoring users and user groups.

a. Select the shared folders to restore on the current device.

Note

This page lists the shared folders recorded in the system configuration file.

Important

- Selected shared folders will be restored according to the configuration recorded in the system configuration file.
- Data in the shared folders is not backed up to, and cannot be restored from, a system configuration file.
- If you restore a shared folder whose recorded path does not exist on the current device, the shared folder will be inaccessible.

Warning

- Shared folders on the current device that are not recorded in the system configuration file will be deleted.
- Unselected shared folders will be removed from the system. Data in unselected folders will be retained but will only be accessible by specifying the original path via a network protocol (such as SSH or Telnet).

b. Click **Next**.
The **Network** page appears.

8. Configure the network settings to restore.
To keep the existing network settings on your device, click **Skip** and go to the next step.

> **Note**
>
> - This step restores certain Network & Virtual Switch settings.
> - Wi-Fi and USB QuickAccess settings will not be restored.
> - To restore network settings, the current device cannot have fewer ports than the device recorded in the system configuration file.

a. Click **Check for IP Conflict**.

> **Tip**
> If an IP address conflict is detected, perform one of the following actions:
>
> - Change the IP address on the other device.
> - Temporarily shut down the other device, restore the system settings on the current device, and then change the IP address on the current device.

b. Click **Next**.
The **Apps** page appears.

9. Configure the applications to restore.
To keep the applications as they are on the current device, click **Skip** and go to the next step.

a. For each application, select an action to perform.

> **Note**
> This page lists all applications recorded in the configuration file. You can choose to take no action, install the latest version of an application, or update an installed application to the latest version.

> **Important**
> Specific application settings (including myQNAPcloud settings) are not backed up to, and cannot be restored from, a system configuration file.
> Only certain network settings in Network & Virtual Switch are backed up and can be restored. For details, see the **Network** page in the wizard.

> **Warning**
> Existing applications on the device that are not on the list will be removed from the system.

b. Click **Next**.
The **Summary** page appears.

10. Review the summary.
11. Optional: Select **Back up current system settings before restoring**.
You can download the backup file to your computer or save it in a folder on the current device.
12. Click **Restore**.
The **Verify Your Identity** window opens.
13. Enter your current account password.
14. Click **OK**.
The **Restart System** window opens.
15. Click **OK**.

The system restores the specified system settings and restarts the device.

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.
- To protect your device from attacks, QNAP recommends disabling the default `admin` account after a system reset or system restore. To disable this account, go to **Control Panel** > **Privileges** > **Users**.

Option	Description
Basic system reset	This resets certain system settings to the default values without deleting the user data stored on the disks. For details, see Basic system reset.
Advanced system reset	This performs a basic system reset and then restores the QTS default settings, deleting all users and user groups. The user data stored on the disks is retained. For details, see Advanced system reset.
Restore factory default settings and format all volumes	This restores the default system settings and formats all disk volumes. For details, see Restoring factory default settings and formatting all volumes.
Reinitialize the NAS	This deletes all data on the disks and reinstalls QTS. For details, see Reinitializing the NAS.

Basic system reset

A basic system reset resets the following settings to the default values without deleting the user data stored on the disks.

Setting	Default Values
System administrator account `admin`	Enabled
Password for the default `admin` account	The Cloud Key of your device without special characters (all letters must be uppercase). For example, if the Cloud Key is Q1234-5678, then the password is Q12345678. **Tip** Your device's Cloud Key is printed on a sticker on your device or in your device's Quick Installation Guide.
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.
   The system performs a basic system reset. After resetting, you can use the default administrator account `admin` to log in to the system.

Advanced system reset

An advanced system reset performs a basic system reset and then restores the QTS default settings, deleting all users and user groups. The user data stored on the disks is retained.

Perform an advanced system reset using one of the following methods.

Method	Steps
Using the reset button	**1.** Power on the NAS. **2.** Press and hold the reset button for 10 seconds. The system performs an advanced system reset. After resetting, you can use the default administrator account `admin` to log in to the system.
Using QTS	**1.** Go to **Control Panel** > **System** > **Backup/Restore** > **Restore to Factory Default**. **2.** Click **Reset Settings**. A password confirmation window appears. **3.** Enter your password. **4.** Click **OK**. **5.** Create a new administrator account. **Note** • If your current account is `admin`, you must perform this step. • If your current account is not `admin`, this step is optional. Click **Create New Administrator** to create a new administrator account. **a.** Specify the following fields: **Username**, **Password**, **Verify Password**. **b.** Optional: Specify **Email (Optional)**. **6.** Choose to restart or shut down the NAS after the system is reset. **7.** Click **Restore**. The system performs an advanced system reset. If you created a new administrator account, then after resetting you must use the new account to log in. Otherwise, use your current account to log in.

Restoring factory default settings and formatting all volumes

Restoring factory default settings and formatting all volumes restores the default system settings and formats all disk volumes.

Warning
Performing this action deletes all data on the device. To retain all files and data on the disks, see Advanced system reset.

1. Go to **Control Panel** > **System** > **Backup/Restore** > **Restore to Factory Default**.
2. Click **Restore Factory Defaults & Format All Volumes**.
   A password confirmation window appears.

3. Enter your password.
4. Click **OK**.
5. Create a new administrator account.

   Note

   - If your current account is `admin`, you must perform this step.
   - If your current account is not `admin`, this step is optional. Click **Create New Administrator** to create a new administrator account.

   a. Specify the following fields: **Username**, **Password**, **Verify Password**.

   b. Optional: Specify **Email (Optional)**.
6. Choose to restart or shut down the NAS after the system is reset.
7. Click **OK**.

The system restores factory default settings and formats all volumes. If you created a new administrator account, after restoring you must use the new account to log in. Otherwise, use your current account to log in.

Reinitializing the NAS

Reinitializing the NAS 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**.
   A password confirmation window appears.
3. Enter your password.
4. Click **OK**.
5. Choose to restart or shut down the NAS after the NAS is reinitialized.
6. Click **OK**.

Restoring the settings of a default shared folder

Shared folders are returned to default settings after resetting a NAS to factory default. You must manually restore the settings of default shared folders.

Important

You must select **Reset Settings** when restoring the device to retain all files and data on your drive.

1. Go to **Control Panel** > **General Settings**.

2. Select the following options:
   - **Enable HTTP compression**
   - **Enable secure connection (HTTPS)**
   - **Do not allow QTS embedding in IFrames**
3. Go to **Control Panel** > **Privilege** > **Shared Folders**.
4. Go to **Others** > **Restore Default Shared Folders**.
   All restored shared folders are listed in the **Shared Folders** table.

Restoring the settings of a non-default shared folder

Non-default shared folders are manually created shared folders. Settings of all shared folders are restored to default settings after resetting the NAS to factory default and must be manually restored.

Important
You must select **Reset Settings** when restoring the device to retain all files and data on your drive.

1. Go to **Control Panel** > **Privilege** > **Shared Folders**.
2. Select **Create** > **Shared Folder**.
3. Enter the **Folder Name**.
4. Select **Enter path manually**.
5. Select the folder path.
6. Select **Create**.
   The non-default shared folders are restored to **File Station**.

Monitoring system status and Resource Monitor

You can monitor the system statuses and consumed resources respectively in **System Status** and **Resource Monitor**.

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, including the server name, model name, CPU, Intel QuickAssist Technology (Intel QAT) support, serial number, BIOS version, memory, multi-channel memory support, firmware version, system up time, time zone, and filename encoding. **Note** • Intel QuickAssist Technology support only appears when it is detected by QTS. • Multi-channel memory support only appears in NAS models with this feature.
Network Status	This screen displays the current network settings of each network interface.
System Service	This screen displays the current status of system services, such as antivirus, networking services, DDNS services, domain controllers, multimedia management, data backup management, surveillance management, remote servers, and VPN servers.
Hardware Information	This screen displays NAS hardware information, such as CPU usage, memory, disk temperature, power supply unit (PSU) status, and system fan speed.

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.

Section	Description
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.
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). You can also sort information in ascending or descending order, column category, show or hide columns, and choose to **Collapse All** or **Expand All** running processes.

4. Privilege Settings

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

Users

Default administrator account

The "admin" user account is the default administrator account. It can configure settings, create users, and install applications. You cannot delete this account. To prevent malicious actors from compromising your system due to easy passwords, QNAP strongly recommends changing the default admin password, creating another administrator account or logging in with an existing administrator account, and disabling the default "admin" account. A new administrator account can perform the same actions as the default administrator account.

The default password of the "admin" account is the Cloud Key of the device. If the system detects that you still use this default password when you log in with the "admin" account, you will be asked to change your password and disable this account to enhance your account security.

You may need this "admin" account to access the system when you perform a system reset with the reset button.

Creating an administrator account

> **Note**
> Create another administrator account before disabling the default admin account.

1. Log in as admin.
2. Go to **Control Panel** > **Privilege** > **Users**.
3. Click **Create** > **Create a User**.
   The **Create a User** window appears.
4. 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.

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 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character.
Password	Specify a password that contains a maximum of 64 ASCII characters. **Note** When re-enabling the "admin" account, you need to change the password if the system detects the password is the default password (Cloud Key or the first MAC address).
Mobile phone (optional)	Specify a phone number that will receive SMS notifications from QTS. **Note** Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
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.

Field	Description
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: • URLs for connecting to the NAS **Tip** You can edit the notification message.

5. Add the user to one or more user groups.
   a. Under **User Group**, click **Edit**.
   b. Select **administrators**.
6. Optional: Specify shared folder permissions for the user.
   a. Under **Shared Folder Permission**, click **Edit**.
   b. Select the shared folder permissions for the user.
   c. Optional: Select **Apply changes to subfolders**.
7. Optional: Specify application privileges for the user.
   a. Under **Edit Application Privilege**, click **Edit**.
   b. Select application permissions for the user.

   By default, administrator accounts can access to all applications.

   Tip
   QNAP recommends denying access to applications and network services that the user does not require. Users without privileges to specific applications will not see it on their main menu.
8. Optional: Set a quota for the user.

   Note
   This option is only available when quotas are enabled.

   a. Under **Quota**, click **Edit**.
   b. Set the quota.
      - **No Limit**: Quota settings do not apply to the user.
      - **Limit disk space to**: Specify a quota for the user.
      - **Use group quotas**: Group quota settings apply to the user.

> **Important**
> Individual quotas may override group quotas. For details, see Quota conflicts.

9. Click **Create**.

Disabling a default administrator account

1. Log in as an administrator.

   > **Note**
   > Do not use the "admin" account.

2. Go to **Control Panel** > **Privilege** > **Users**.
3. Click .
   The **Edit Account Profile** window opens.
4. Select **Disable this account**.
5. Optional: Select one of the following options.

Option	Description
Now	Disables the account immediately.
Expiry date	Disables the account on the specified date.

6. Click **OK**.

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.

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 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character.
Password	Specify a password that contains a maximum of 64 ASCII characters.
Verify Password	Enter the password again.
Mobile phone (optional)	Specify a phone number that will receive SMS notifications from QTS. **Note** Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
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.
UID	A UID is automatically generated for the user. You can also click  to specify a custom UID.
User must change password at first logon	When selected, the user must change the password when logging in for the first time.

Field	Description
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** You can edit the notification message.

4. Optional: Add the user to one or more user groups.
   a. Under **User Group**, click **Edit**.
   b. Select one or more user groups.
5. Optional: Specify shared folder permissions for the user.
   a. Under **Shared Folder Permission**, click **Edit**.
   b. Select the shared folder permissions for the user.
   c. Optional: Select **Apply changes to subfolders**.
6. Optional: Specify application privileges for the user.
   a. Under **Edit Application Privilege**, click **Edit**.
   b. Select application permissions for the user.

   Tip
   QNAP recommends denying access to applications and network services that the user does not require. Users without privileges to specific applications will not see it on their main menu.
7. Optional: Set a quota for the user.

   Note
   This option is only available when quotas are enabled.

   a. Under **Quota**, click **Edit**.
   b. Set the quota.
      - **No Limit**: Quota settings do not apply to the user.
      - **Limit disk space to**: Specify a quota for the user.
      - **Use group quotas**: Group quota settings apply to the user.

> **Note**
> Individual quotas may override group quotas. For details, see Quota conflicts.

8. Click **Create**.

Creating multiple users

1. Go to **Control Panel** > **Privilege** > **Users**.
2. Click **Create** > **Create Multiple Users**.
   The **Multiple Users Creation Wizard** appears.
3. Click **Next**.
4. 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: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([ ]), curly brackets ({}), slash (\), vertical bar (|), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question mark (?), percent sign (%), dollar sign ($), and the space character. 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 (1–4095). Example: `5`
Password	Specify a password that contains a maximum of 64 ASCII characters.

Field	Description
Verify Password	Enter the password again.
Show password	Select this option to see the password.

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**.
6. Specify the following information.

Field	Description
Disallow the user to change password	When selected, QTS prevents the user from changing the password.
User must change password at first logon	When selected, the user must change the password when logging in for the first time.
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**.

7. Click **Next**.
The **Create Private Network Share** screen appears.
8. 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.

Field	Description
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**.

9. Click **Next**.
   QTS creates the user accounts and adds them to the displayed user list.
10. 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

1. Create a new file in a text editor.
2. Specify user information in the following format.
   `Username`,`Password`,`Quota (MB)`,`Group Name`, `Email`, and `User Description`.

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,john@email.com,Sales Manager
Jane,9fjwbx,150,Marketing,jane@email.com
,Marketing Specialist
Mary,f9xn3ns,390,RD,mary@email.com,Senior Engineer
```

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 user file

1. Create a new workbook in a spreadsheet editor.
2. Specify user information in the following format.
   - column A: `Username`
   - column B: `Password`
   - column C: `Quota (MB)`
   - column D: `Group name`
   - Column E: `Email`
   - Column F: `User Description`

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	E	F
1	John	s8fk4b	100	Sales	john@email.com	Sales Manager
2	Jane	9fjwbx	150	Marketing	jane@email.com	Marketing Specialist
3	Mary	f9xn3ns	390	R&D	mary@email.com	Senior Engineer

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.

Importing users

1. Go to **Control Panel** > **Privilege** > **Users**.
2. Click **Create** > **Import/Export Users**.
   The **Import/Export Users** window appears.
3. Select **Import user and user group settings**.
4. 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.

Field	Description
Overwrite duplicate users	When selected, QTS overwrites existing user accounts that have duplicates on the imported user account list.
User must change the password at first logon	When selected, users will be asked to change their password the next time they log into QTS.

5. 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

Important
Although non-administrators with delegated roles of "System Management" or "User and Group Management" can manage and modify the account settings of other non-administrators, they cannot see or edit their own accounts in the user list, nor can they see or edit administrator accounts.

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 contains a maximum of 64 ASCII characters. **Note** For "admin" accounts, the new password cannot be the default password (Cloud Key or the first MAC address). **c.** Verify the password. **d.** Click **Apply**.

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: • **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**. **Note** QNAP recommends users to create a new administrator account and disable the "admin" account. To create an administrator account, see Creating an administrator account. **c.** Modify the quota for the user. **Note** This option is only available when quotas are enabled. • **No Limit**: Quota settings do not apply to the user. • **Set user's quota limitation**: Specify a quota for the user. • **User group quotas**: Apply user group quota to the user. **Important** Individual quotas may override group quotas. **d.** Optional: Click **Disable 2-step Verification**. **Note** For details, see Disabling 2-step verification. **e.** Click **OK**.

Task	User Action
Edit user group membership	**a.** Under **Action**, click  . The **Edit User's Groups** window appears. **b.** Select or deselect user groups. **c.** Click **Apply**.
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. **c.** Optional: Select **Apply changes to subfolders**. **d.** Click **Apply**.
Edit application privileges	**a.** Under **Action**, click  . The **Edit Application Privileges** window appears. **b.** Select the applications that the user is allowed to access. **c.** Click **Apply**. **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.

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. When a home folder is created, the user's home folder appears as a shared folder called `home`. Users can access their home folder through Microsoft networking, FTP, and File Station.

All user home folders are located in the `homes` shared folder. By default, only administrators can access this folder. If home folders are disabled, home folders become inaccessible to users. However, the folders and files they contain are not deleted from the NAS. Administrators can still access the `homes` folder and each user's home 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.
   Home folders are stored on the selected volume.
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 **User group name**.
   The user group name can contain 1 to 128 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 (-)
4. Optional: Specify a description that contains a maxiumum of 128 characters.
5. Optional: Add users to the user group.
   a. Under **Assign users to this group**, click **Edit**.
   b. Select one or more users.
6. Optional: 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.
7. Optional: Set a quota for the user group.

   Note
   This option is only available when quotas are enabled.
   For details, see Enabling quotas.

   a. Under **Quota**, click **Edit**.
   b. Set the quota.
      - **No Limit**: Quota settings do not apply to the user group.
      - **Limit disk space to**: Specify a quota for the user group.

      Important
      Individual quotas may override group quotas.
      For details, see Quota conflicts.
8. Click **Create**.
   A dialog box appears.
9. Choose whether group quotas will be applied to users in the group.

Option	Description
Yes	Applies group quota settings to each user in the group.

Option	Description
No	Retains individual quota settings for users in the group.

For details on group quota settings, see Quota conflicts.

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 user group details	**a.** Under **Action**, click  . The **View Group Details** window appears. **b.** Modify the description. **c.** Modify the quota. **Note** • You cannot modify the quota in the default user group. • This option is only available when quotas are enabled. For details, see Enabling quotas. • **No Limit**: Quota settings do not apply to the user group. • **Limit disk space to**: Specify a quota for the user group. **Important** Individual quotas may override group quotas. For details, see Quota conflicts. **d.** Click **OK**.
Edit user group members	**a.** Under **Action**, click  . The **Edit User Group** window appears. **b.** Select or deselect users. **c.** Click **Apply**.

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. **c.** Click **Apply**. **Important** Group-level permissions may override user-level permissions. For details, see Conflicts in shared folder permissions.

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**.

Delegated administration

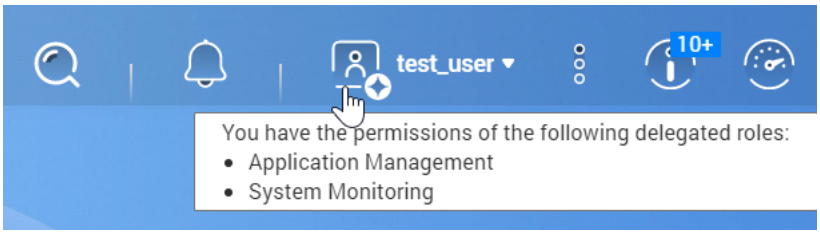
Delegated Administration allows administrators to assign one or more pre-defined roles to non-administrator users or groups. With delegated roles, non-administrator users can help manage system resources and perform routine tasks, such as updating apps, monitoring CPU usage, and backing up important data. This reduces the workload of system administrators and provides better flexibility and efficiency for your organization.

Delegated roles and permission restrictions

Overview

Administrators assign one or more delegated roles to up to 32 local/domains users and 32 local/domain groups. Users have the privileges of the delegated roles that are assigned to them and their groups.

Users can see their assigned roles by hovering over their user name on the Desktop task bar.



Users with delegated roles can only access settings associated with their roles. For example, users assigned the Application Management and System Monitoring roles can only access App Center, Resource Monitor, and Desktop Dashboard, but have no access to other system settings.

Important

To ensure system security and functionality, non-administrators with delegated roles have the following general restrictions.

- Unable to manage the "administrators" group or its members
- Unable to change their own account settings
- Can only grant or change permissions that are within the scope of their own privileges.
  - For example, if a delegated users has read-only access to a shared folder, this user can only grant other users read-only permissions or deny them access to this shared folder.
- May only have limited or no access to certain sensitive settings or functions when performing administrative tasks or when using applications and services, even with associated roles

Delegated Roles

For details on each delegated role and their respective restrictions, see the following table.

Delegated Role	Permissions	Restrictions
System Management	This role has the permissions of all delegated roles. This role also has permission to use the following applications or services: QuLog Center, Notification Center, Network & Virtual Switch, Security Counselor, License Center, QuFTP Service, Malware Remover, Multimedia Console, Control Panel, Storage & Snapshots, and iSCSI & Fibre Channel.	Unable to access the following settings in Control Panel: Delegated Administration, System Restore, Telnet/SSH, and Recycle Bin

Delegated Role	Permissions	Restrictions
Application Management	This role has permission to manage apps in the App Center.	• Unable to manually install apps or configure settings in the App Center • Unable to open apps that are only accessible to administrators
Access Management	This role has permission to configure security settings in Control Panel and to use QuFirewall.	-
System Monitoring	This role has permission to monitor the system in Resource Monitor and Desktop Dashboard.	-
User and Group Management	This role has permission to create, edit, and delete local users and groups. This role can also edit domain users and groups.	• Unable to create a user or a group if the delegated user is not assigned the Shared Folder Management role • Unable to manage the shared folder access rights of users or groups if the delegated user is not assigned the Shared Folder Management role
Shared Folder Management	This role has permission to create, edit, and delete shared folders.	• Unable to access the settings of Advanced Permissions or Folder Aggregation • Unable to create a shared folder if the delegated user is not assigned the User and Group Management role. • Unable to create a snapshot shared folder
Backup Management	This role has permission to use Hybrid Backup Sync and Hyper Data Protector. In addition, this role also has the permissions of the Shared Folder Management role.	-

Delegated Role	Permissions	Restrictions
Backup Operation	This role has permission to help administrators monitor, manage, and execute backup tasks in Hybrid Backup Sync and Hyper Data Protector but cannot overwrite or delete existing backup data. In addition, this role also has the permissions of the Shared Folder Management role.	-

Assigning delegated roles to users

Administrators can assign one or more delegated roles to non-administrator users and groups.

Important
Assigning the System Management role grants the permissions of all other roles.

1. Log in to QTS as administrator.
2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Select a delegated role from the role list.
4. Select a user type or group type from the drop-down list.
   - Local users
   - Local groups
   - Domain users
   - Domain groups
5. Select one or more users or groups to which you want to assign this delegated role.

   Tip
   If you have numerous users or groups on the list, you can type a user name or group name in the search box to quickly find your target.

   In the **Delegated Roles** column, QTS instantly displays the delegated role that you have assigned to the selected user or group. Note that you still need to apply changes, otherwise this delegation would not take effect.
6. Optional: Assign additional delegated roles.
7. Click **Apply**.

Removing delegated roles from users

Administrators can remove delegated roles from non-administrator users to withdraw their permissions. You can remove only one or more delegated roles.

Important

Given that System Management role covers all other delegated roles, QTS does not allow you to remove a smaller role from a user who has been assigned the System Management role. You should first remove the System Management role from this user and then adjust role assignment according to your needs.

1. Log in to QTS as administrator.
2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Select a delegated role from the role list.
4. Select a user type or group type from the drop-down list.
   - Local users
   - Local groups
   - Domain users
   - Domain groups
5. Deselect one or more users or groups from which you want to remove this delegated role.

   Tip

   If you have numerous users or groups on the list, you can type a user name or group name in the search box to quickly find your target.

   In the **Delegated Roles** column, QTS instantly displays the delegated role that are currently assigned to the selected user or group. Note that you still need to apply changes, otherwise this delegation would not take effect.
6. Optional: Remove more deleted roles from users or groups if needed.
7. Click **Apply**.

Viewing user permissions

Permission Viewer displays a summary of current role assignments in Delegated Administration, allowing you to quickly understand which permissions have been granted to non-administrators.

Note

If no delegated role has been assigned, Permission Viewer displays an empty list.

1. Log in to QTS as administrator.

2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Click **Permission Viewer**.
   The **Permission Viewer** window appears.
4. Select a viewing mode.

Viewing Mode	Description
By users and groups	This mode lists delegated roles assigned to each user and group. In this viewing mode, you can also choose to view all users and groups or only view a specific user/group type.
By delegated roles	This mode lists every user and group assigned to each delegated role.

Exporting a delegation list

You can back up your settings by exporting the current delegation settings in CSV format.

Tip
In the exported CSV file, each row represents a user or group, and each column represents a delegated role. You can check the intersection of each row and column to understand each permission status. 1 indicates that the delegated role is assigned, and 0 indicates the delegated role is not assigned.

1. Log in to QTS as administrator.
2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Click **Permission Viewer**.
4. Click **Export**.

QTS exports and downloads a CSV file to your computer. You can import this CSV file later to restore your settings.

Importing a delegation list

You can restore previous delegation settings by importing a valid CSV file.

Tip
In a valid CSV file, each row represents a user or group, and each column represents a delegated role. You can check the intersection of each row and column to understand each permission status. 1 indicates that the delegated role is assigned, and 0 indicates the delegated role is not assigned.

1. Log in to QTS as administrator.

2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Click **Permission Viewer**.
4. Click **Import**.
5. Click **Browse**.
6. Select a CSV file to import.
7. Click **Import**.

QTS imports delegation settings from the selected CVS file and apply settings. If you do not see the new delegation settings, restart Control Panel and then check again.

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
You cannot delete or modify certain properties of default shared folders.

Folder	Description
Multimedia	This is the default folder for multimedia apps. The folder stores multimedia content such as photos, videos, and music. You can manage this folder in the Multimedia Console utility in **Control Panel** > **Applications**.
Public	This folder can be used by any user account. The default permission of this folder is 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** > **Applications** > **Web Server**. **Note** You must enable **Web Server** automatically to create this default shared folder.

Restoring default shared folders

You can restore default shared folders that were deleted.

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

2. Click **Restore Default Shared Folders**.
   A warning message appears.
3. Click **OK**.

QTS restores the default shared folders.

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 or end with a space • 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 path automatically**: Creates a new root folder on the selected volume using the specified shared folder name. • **Enter path manually**: Select an existing folder as the root folder.

5. Optional: Enable folder encryption.

   a. Under **Folder Encryption**, select **Encryption**.
   Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.

   b. 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. **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, all data will become inaccessible.

6. Click **Next**.
7. Optional: Specify the access permissions for users.
   For details, see Shared folder permissions.
8. Click **Next**.
9. Optional: Configure properties.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Hide network drive	Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder.

Option	Description
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	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is 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. **Important** • If space in the folder is insufficient when starting a new Time Machine backup, QTS automatically deletes the oldest Time Machine backup in the folder to free up space. • You should disable **Enable Network Recycle Bin** when **Set this folder as the Time Machine backup folder (macOS)** is selected to prevent automatically deleted Time Machine backups from filling the recycle bin.
Instant sync to disks when requested by SMB clients	Enabling this option allows the system to immediately synchronize data to disks when requested by SMB clients and therefore provides better data integrity. Disabling this option improves I/O performance but may increase the risk of data loss or corruption in the event of power outage or system failure.

10. Click **Finish**.

Tip
Hovering your mouse underneath the columns **Size**, **Folders**, and **Files** displays the shared folder's size, number of folders, number of files, and last update time.

Editing shared folder properties

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. Modify any of the following settings.

Important
A HybridMount shared folder can only modify comments, set the shared folder as a backup folder, and enable access-based share enumeration and access-based enumeration.

Setting	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 which 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. **Tip** You can also enable auto-tiering from the **Shared Folders** screen.
Path	View the folder path.
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.

Setting	Description
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. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable write-only access on FTP connection	When enabled, only the admin has read and write access to the shared folder. Other users will only be able to write to the folder.
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.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is 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.

Setting	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. **Important** • If space in the folder is insufficient when starting a new Time Machine backup, QTS automatically deletes the oldest Time Machine backup in the folder to free up space. • You should disable **Enable Network Recycle Bin** when **Set this folder as the Time Machine backup folder (macOS)** is selected to prevent automatically deleted Time Machine backups from filling the recycle bin.
Instant sync to disks when requested by SMB clients	Enabling this option allows the system to immediately synchronize data to disks when requested by SMB clients and therefore provides better data integrity. Disabling this option improves I/O performance but may increase the risk of data loss or corruption in the event of power outage or system failure.

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 confirmation message appears.
4. Optional: Select **Also delete the data**.
5. Click **Yes**.

Enabling daily updates for shared folders

You can set a time for QTS to check the size and the number of folders and files for all of your shared folders.

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Shared Folder** > **Others**.
2. Click **Settings**.
   The **Settings** window opens.
3. Select **Enable daily updates for shared folder size and the number of folders and files**.
4. Select a time.
5. Click **Apply**.

Snapshot shared folders

A snapshot shared folder is a shared folder created on a dedicated volume and 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: " + = / \ : | * ? < > ; [ ] % ` '.

Field	Description
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Storage Pool	Specify the storage pool where the shared folder will be created.
Space Allocation	Select one of the following space allocation options: • **Thick provisioning** • **Thin provisioning**
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. This setting is only available if you select a Qtier-enabled storage pool. **Tip** You 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. Click **Next**.
5. Optional: Specify the access permissions for users.
   For details, see Shared folder permissions.
6. Optional: Configure properties.
   For details, see Creating a shared folder.
7. Click **Finish**.

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 the storage pool doesn't have enough space for the snapshot shared folder, the **Increase Pool Free Space** screen appears.

Option	User Action
Release unused pool guaranteed snapshot space	**Note** This option is only available if guaranteed snapshot space has been allocated to the storage pool. **a.** Click **Edit**. 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 **Execute**. 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
Delete older snapshots	**a.** Select a volume. **b.** Click **Manage**. The **Snapshot Manager** window opens. **c.** Optional: Click ☰ to change to list view. **d.** Select one or more older snapshots to delete. **e.** Click  . **f.** Close the window. **g.** Optional: Repeat this process on another volume.
Convert a thick volume to a thin volume to release unused space in the volume	**Note** This option is only available if the storage pool contains a thick volume. **a.** Select a volume to convert. **b.** Click **Execute**. The **Convert to Thin Volume** window appears. **Warning** Converting a volume deletes all existing snapshots on the volume. **c.** Click **Apply.** QTS converts the volume.
Expand current storage pool by adding disks or a new RAID group	**a.** Click **Expand**. The **Expand Storage Pool Wizard** window opens. **b.** Select one of the following options and complete the wizard: • **Create and add a new RAID group** For details, see Expanding a storage pool by adding a new RAID group. • **Add new disk(s) to an existing RAID group** For details, see Expanding a storage pool by adding disks to a RAID group.

7. Configure the snapshot shared folder.

Field	Description
Qtier Auto Tiering	When enabled, Qtier performs auto-tiering on data in the folder. This setting is only available if you select a Qtier-enabled storage pool. **Tip** You can also enable auto-tiering from the **Shared Folders** screen.
Space Allocation	Select one of the following space allocation options: • **Thick provisioning** • **Thin provisioning**
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. By default, most NAS models support up to 256 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 Recycle Bin folders: Number of supported ISO image files = 256 − 6 (default shared folders) − (number of 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.

Field	Description
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.	-
	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. **Note** If a user creates a shared link to a folder they no longer have RW permissions to, anyone with that shared link cannot access the folder.
Deny	The user or user group cannot read or write files in the shared folder.

Editing shared folder permissions

Note
Users with the delegated role of "Shared Folder Management" cannot view or edit the settings of NFS host access and Microsoft networking host access.

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. Specify 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.	**a.** Select **Access right** to enable NFS access rights. **Note** You can't select this for folders mounted by HybridMount using SMB file protocol. These folders do not support NFS host access. However, you can still access the NFS host access page. **b.** Under **Host / IP / Network**, enter an IP address or domain name. **c.** Optional: Add an NFS host. Under **Allowed IP Address or Domain Name**, click **Add**. QTS adds an entry to the list. **d.** Optional: Delete an NFS host. **1.** Select an NFS host from the list. **2.** Click **Delete**.
Microsoft Networking host access	Specify which computers can access shared folders through Microsoft Networking.	**a.** Add a Microsoft Networking host. **1.** Click **Add**. QTS adds an entry to the list. **2.** Under **Host / IP / Network**, enter an IP address or domain name. **b.** Optional: Delete a Microsoft Networking host. **1.** Select a Microsoft Networking host from the list. **2.** Click **Delete**.

6. Click **Apply**.

Configuring advanced folder permissions

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Advanced Permissions**.

2. 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.

1. No Access/Deny
2. 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

User Permission	User Group Permission	Actual Permission
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

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 50 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.

Task	User Action
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.

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 Configuring encryption settings.

   The **Folder Encryption** window appears.

6. Review the information.
7. Click **Yes**.

Configuring encryption settings

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 encryption key.
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 locks the folder. **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

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Shared Folder**.
2. Locate a locked shared folder.

3. Under **Action**, click  .
   The **Unlock Folder** window appears.
4. 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.

5. Click **OK**.

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.

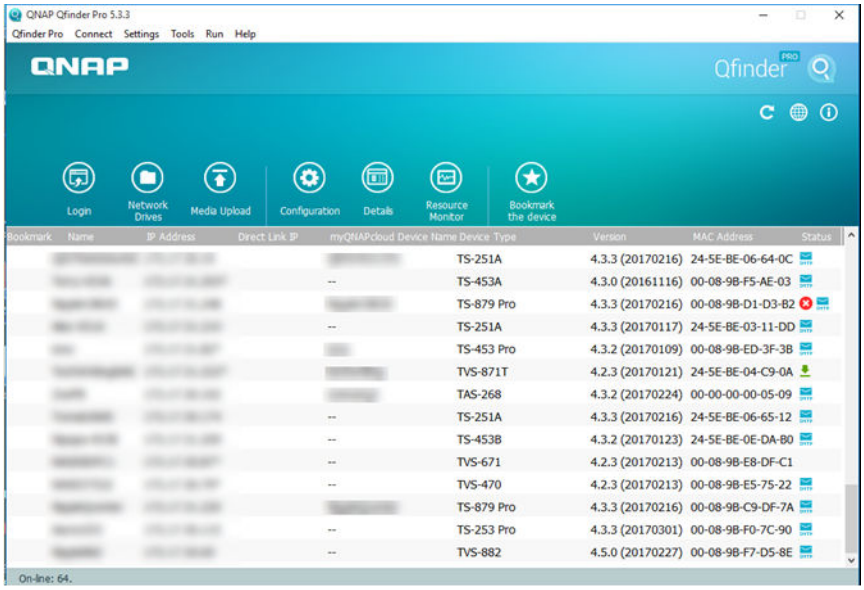
To download Qfinder Pro, go to https://www.qnap.com/utilities.

Mapping a shared folder on a Windows computer

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

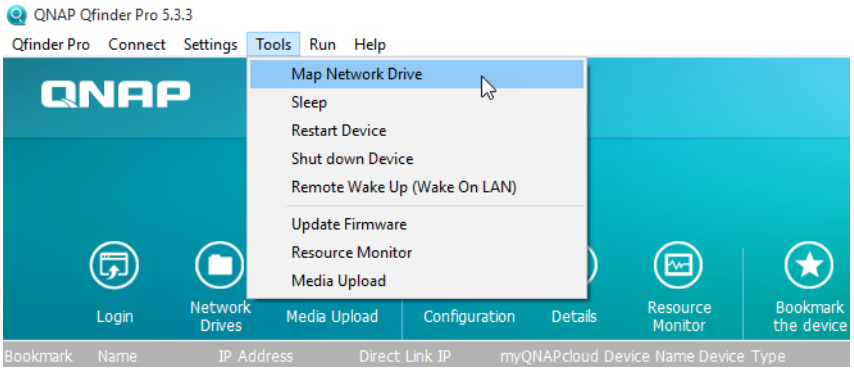
1. Power on the NAS.
2. Connect the NAS to your local area network.

3. Open **Qfinder Pro**.
   Qfinder Pro displays all QNAP NAS devices in your local area network.



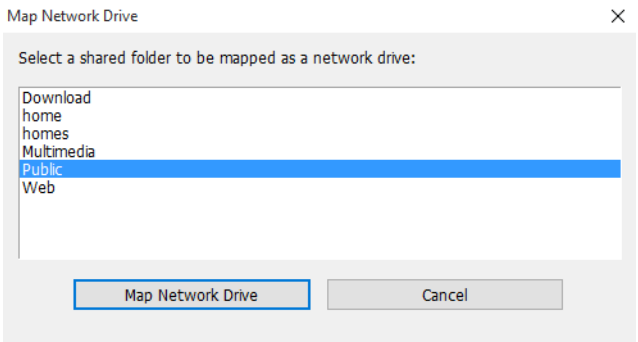
4. Select the NAS where the shared folder is located.

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



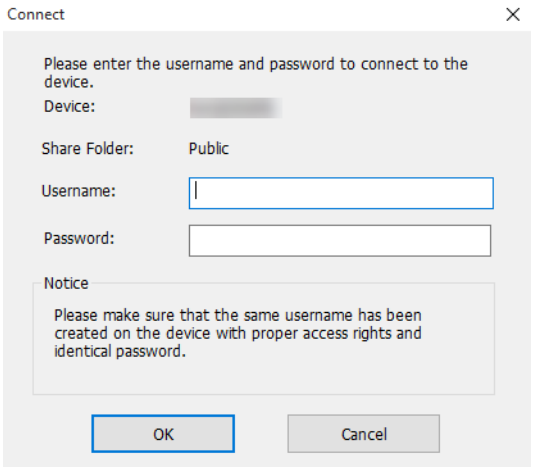
6. Select a shared folder.

7. Click **Map Network Drive**.

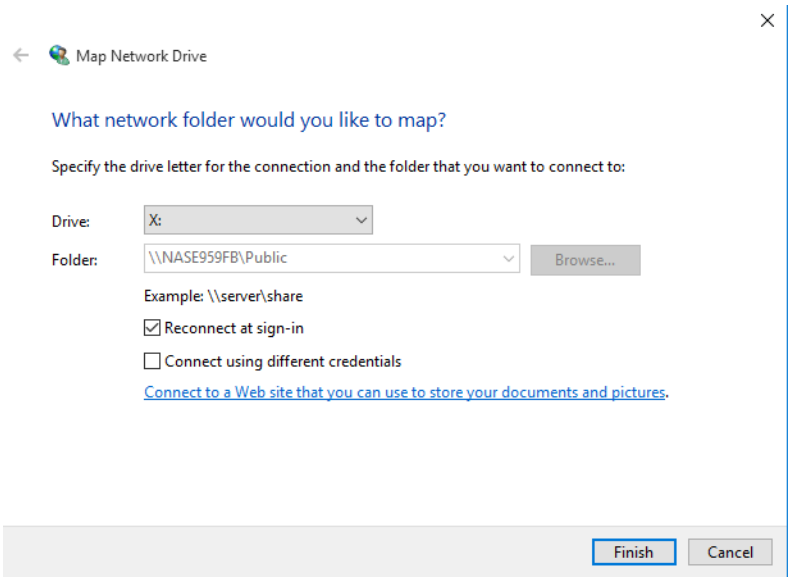


8. Specify your QTS username and password.

9. Click **OK**.



10. Specify the following information.



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.

Field	Description
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.

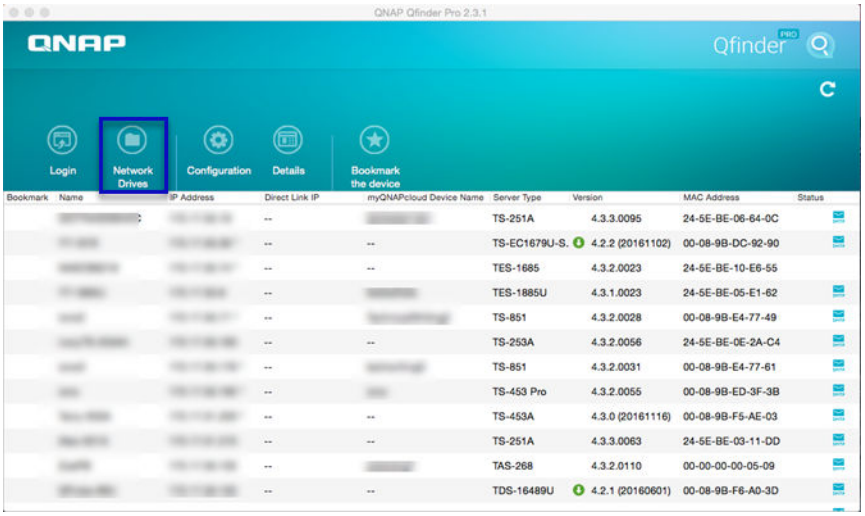
11. Click **Finish**.

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

Mounting a shared folder on a Mac computer

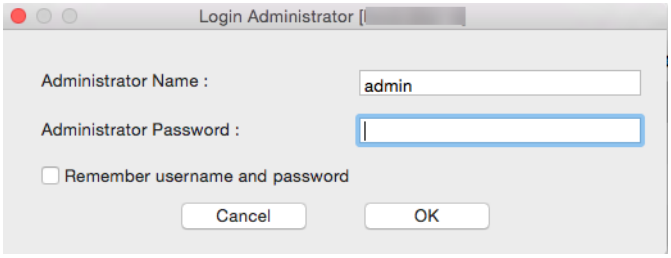
Before mounting a shared folder, ensure that you have Qfinder Pro installed on your Mac computer.

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**.



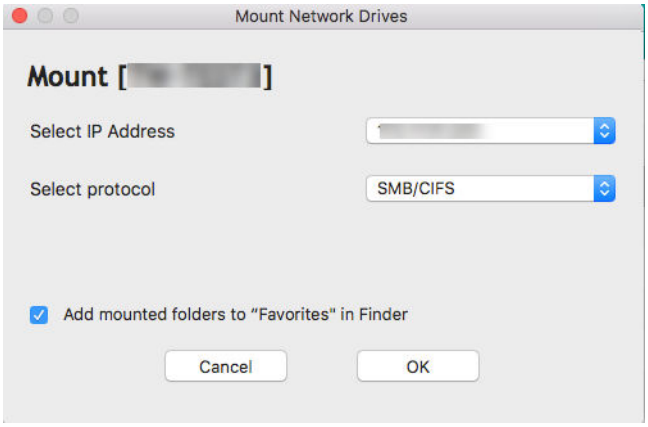
6. Specify your QTS username and password.

7. Click **OK**.



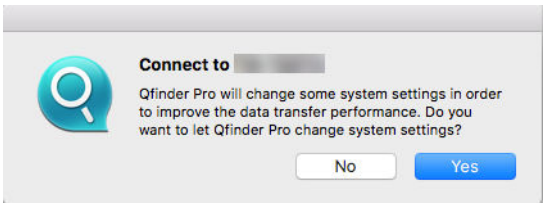
The **Mount Network Drives** window opens.

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

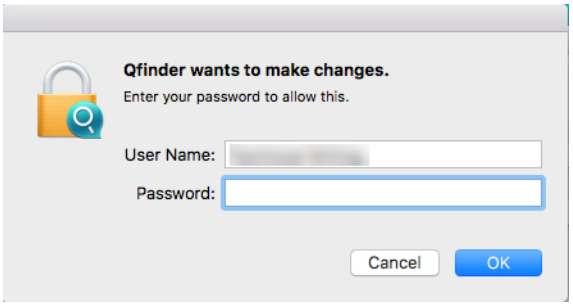


A confirmation message appears.

10. Click **Yes**.

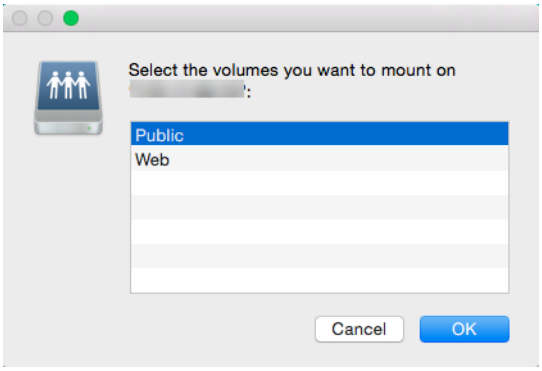


11. Specify your Mac username and password.
12. Click **OK**.



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.

Quota

You can enable quotas (in MB or GB) for users and user groups to help manage storage space. When quotas are enabled, QTS prevents users from saving data to the NAS after the quota is reached. By default, quotas are not enabled for users.

QTS provides three types of quota settings.

Type	Description
Individual	Set quotas for individual users. Go to **Control Panel** > **Privilege** > **Users** to edit user quotas. For details, see Modifying user account information.

Type	Description
Group	Set quotas at the group level. Setting a group quota applies the quota to each user in the group. Go to **Control Panel** > **Privilege** > **User Groups** to edit group quotas. For details, see Modifying user group information.
All users	When enabled, the quota is applied to both new and existing users. Go to **Control Panel** > **Privilege** > **Quota** to enable quotas. For details, see Enabling quotas.

Note
Quotas are applied per volume and are not shared across volumes.

Important
Individual quotas may override group quotas.
For details, see Quota conflicts.

Tip
You can export quota settings to a CSV file to use as a reference.
For details, see Exporting quota settings.

Enabling quotas

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

   Note
   The all users quota must be between 100 MB and 128 TB.

4. Click **Apply**.
   QTS displays the quota settings for Local Users.

Editing quota settings

1. Go to **Control Panel** > **Privilege** > **Quota**.
2. Select the type of user or group.
   - **Local Users**
   - **Domain Users**

- **Local Groups**
- **Domain Groups**

> **Tip**
> By default, the **Quota** screen displays Local Users.

3. Select a user or group.
4. Click **Edit**.
   The **Quota** window appears.
5. Set a quota for the user or group.
   - **No Limit**: Quota settings do not apply to the user or group.
   - **Limit disk space to**: Specify a quota for the user or group.

     > **Note**
     > The quota must be between 100 MB and 128 TB.

   - **Use group quotas**: Group quota settings apply to the user.

   > **Important**
   > Individual quotas may override group quotas.
   > For details, see Quota conflicts.

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.

Quota conflicts

QTS uses the following hierarchy to resolve quota conflicts.

1. Individual quota
2. Group quota
3. All users quota

The following table describes the possible scenarios for different combinations of user quotas and group quotas.

- The **User Quota** column shows the quota setting that is applied to the user individually.
- The **Group Quota** column shows whether the user belongs to any groups.
- The **Actual Quota** column shows the actual quota setting that is applied to the user.

User Quota	Group Quota	Actual Quota
No limit	Yes	No limit
	No	No limit
Individual	Yes	Individual quota
	No	Individual quota
Use group quotas	Yes	Group quota
	No	All users quota

Note
If a user belongs to multiple groups with group quotas, the highest group quota applies to the user.

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 2008 R2, 2012, 2012 R2, 2016, 2019, and 2022.

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.

Option	Description
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 domain name 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. Select a server signing option.
    - **Sign if client agrees**
      SMB signing is recommended but not enforced on the client device.
    - **Enforce signing**
      Clients must digitally sign all the communications.
    - **Sign according o selected SMB version**

SMB signing is disabled if the client selects SMBv1. If SMBv2 or SMBv3 is enabled on the client device, SMB signing is recommended but not enforced.

12. Click **Join**.
    The NAS joins the domain.
13. 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.
- 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.
- You have specified the IP address of the WINS server that you use for name resolution.

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. Select a server signing option.
   - **Sign if client agrees**

SMB signing is recommended but not enforced on the client device.

- **Enforce signing**
  Clients must digitally sign all the communications.
- **Sign according o selected SMB version**
  SMB signing is disabled if the client selects SMBv1. If SMBv2 or SMBv3 is enabled on the client device, SMB signing is recommended but not enforced.

6. 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.
2019	Go to **Control Panel** > **System and Security** > **System** in Windows. 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**.

Azure Single Sign-On (SSO)

Single Sign-On (SSO) is a holistic approach to authenticate users when signing on to applications on Azure. If you enable SSO, a user only needs one login credential to access multiple applications, irrespective of the platform, domain, or technology used. Without SSO, a user needs a separate credential to access each application. The NAS supports SSO. Depending on which domain service the NAS joins, the device will synchronize the domain account information with the appropriate service.

Note
Azure Active Directory (Azure AD) has been renamed as Microsoft Entra ID. This nomenclature change aligns with Microsoft's broader Entra platform for identity and access management.
For details, see New name for Azure Active Directory.

Enabling Azure Single Sign-On

Before starting this task, ensure that you create an application registration. For details, see https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal. The user interface on Microsoft Azure is subject to change without notice.

Important

You must first complete the following steps before enabling SSO.

- Ensure that your NAS has an x86 (Intel or AMD) processor.
- Configure Azure site-to-site VPN. For details, visit https://learn.microsoft.com/azure/vpn-gateway/tutorial-site-to-site-portal.
  You can also add a custom domain name using the Azure AD portal for the on-premise Windows AD. For details, visit https://learn.microsoft.com/entra/fundamentals/add-custom-domain.
- Configure Azure AD Domain service. For details, see the following:
  - Configuring AD authentication using the Quick Configuration Wizard
  - Configuring AD authentication manually

Note

If you want to enable SSO on more than one NAS, you must repeat all of these steps on each NAS.

1. Go to **Control Panel** > **Privilege** > **Domain Security** > **SSO**.
2. Select **Enable Azure Single Sign-On (SSO)**.
3. Specify **Client ID**.
   For details, visit https://learn.microsoft.com/entra/identity-platform/howto-create-service-principal-portal.

   Note

   The Client ID is also known as an Application ID.
4. Specify **Tenant ID**.
   For details, visit https://learn.microsoft.com/entra/fundamentals/how-to-find-tenant.
5. Specify **Reply URLs**.

   Note

   - Microsoft uses **reply URL** and **redirect URI** interchangeably.
   - To locate the base redirect URI, refer to https://learn.microsoft.com/entra/identity-platform/reply-url.

   a. Sign in as an administrator at https://portal.azure.com/#home.
   b. In the search bar, enter `App registrations`.
   c. Click **App registrations**.
   d. Locate your application.

e. Click your application.
The **Overview** page appears.

f. Locate the reply URL (redirect URI).

g. Copy the reply URL to the clipboard.

h. Append `:8080/cgi-bin` to the end of the reply URL.

i. Paste the URL into the **Reply URLs** field in the NAS interface.

6. Specify the **Public key**.

Note

- The public key must be a PEM file.
- You can convert a CA certificate to a public key using a Linux environment or an OpenSSL.

7. Click **Apply**.

Note
Your NAS login screen changes to include an Azure SSO login option.

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 Server Type	Fields	User Action
Remote 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 636. Older versions of LDAP servers normally use this port.
	Base DN	Specify the LDAP domain. Example: `dc=mydomain,dc=local`
	Root DN	Specify the LDAP root user. Example: `cn=admin, dc=mydomain,dc=local`
	Password	Specify the root user password.
	Users Base DN	Specify the Organizational unit (OU) where users are stored. Example: `ou=people,dc=mydomain,dc=local`
	Group Base DN	Specify the OU where groups are stored. Example: `ou=group,dc=mydomain,dc=local`
	Current Samba ID	-
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	-	-
IBM Lotus Domino	This server type includes the same fields as **Remote LDAP server**, in addition to the following:	

LDAP Server Type	Fields	User Action
IBM Lotus Domino	**uidNumber**	Specify the uid number. Select **HASH**.
	gidNumber	Specify the gid number. Select **HASH**.

5. Click **Apply**.
   The **LDAP authentication options** window appears.
6. 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.

7. Click **Finish**.

LDAP authentication options

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

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	**a.** Under **Action**, click  . The **Edit Account Profile** window appears. **b.** Edit the user quota. **Note** User quotas must be enabled for this option to appear. For details, see Enabling quotas.
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.

Tip

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

5. Click **Apply**.

Managing AD and LDAP user groups

1. Go to **Control Panel** > **Privilege** > **User Groups**.

2. Select **Domain Groups**.
   QTS displays the list of domain user groups.
3. Locate a user group.
4. 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.

5. 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.
To enable **Domain Controller**, you must first enable Advanced Folder Permissions by going to **Control Panel** > **Privilege** > **Shared Folders** > **Advanced Permissions**.

Note

When you enable the domain controller, FTP and AFP services will be restarted.

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**	**Domain**	Specify the domain.

Domain Controller Mode	Field	Description
• **Read-Only Domain Controller**	**Domain DNS IP**	Specify the domain DNS IP.
	Administrator Account	Specify the administrator account name.
	Administrator Password	Specify the administrator password.

5. Select the server signature rule for the domain.

Option	Description
Optional	SMB signing is offered but not enforced. Clients can choose whether to use SMB signing or not.
Required	SMB signing is required.
Optional for SMBv2 and SMBv3	SMB signing is disabled for SMB 1. For SMB 2 and above, this option behaves the same as **Optional**.

6. 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.

Domain User Account	Description
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`.

Field	Description
Number of Users	Specify a number between 1 and 4095. This number signifies the number of accounts that will be created.
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.

5. Click **Create**.
   QTS creates the accounts and adds them to the list of domain users.
6. 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

1. Create a new file in a text editor.

2. 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	**a.** Under **Action**, click  . The **Edit computer properties** window appears. **b.** Edit the **Description** or **Location**. For details, see Creating a computer account.

Task	User Action
Edit user group membership	a. Under **Action**, click  . The **Edit User Groups** window appears. b. Select or deselect user groups. For details, see Domain user groups. c. Click **Next**.

4. Click **Finish**.

Editing computer account shared folder permissions

1. Go to **Control Panel** > **Privilege** > **Domain Conroller** > **Computers**.
2. Locate a computer account.
3. Under **Action**, click  .
   The **Edit Shared Folder Permission** window appears.
4. Edit the computer account's permissions for each shared folder.
   For details, see Shared folder permissions.
5. Click **Apply**.

Deleting computer accounts

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Computers**.
2. Select the accounts to delete.

   Note
   The host computer account cannot be deleted.

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

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 `administrator`.
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.

Task	User Action
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 `administrator`.
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 `administrator`.
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 `administrator`.
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**.

5. Services

QTS provides various services to facilitate your work and device management. You can configure these settings according to your needs.

Antivirus

To ensure your NAS is protected from malicious attacks, you can scan the NAS manually or on recurring schedules. Antivirus will delete, quarantine, or report files infected by viruses, malware, trojans, or other threats.

Enabling antivirus

Important
You must install and start the ClamAV application before enabling the antivirus function.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Overview**.
3. Select **Enable antivirus**.
4. Optional: Update the antivirus with one of the following methods.

Option	User Action
Update now	Click **Update now**. The system immediately updates the antivirus.
Update automatically	**a.** Select **Check and update automatically**. **b.** Specify the frequency. The system automatically checks for antivirus updates on the specified date.

Option	User Action
Update manually	**a.** Click **Browse**. An upload window appears. **b.** Select a virus database file (.cvd) to upload. **Tip** You can download the latest ClamAV virus database file from http://www.clamav.net. **c.** Click **Import**.

5. Click **Apply**.

QTS enables antivirus.

Scanning shared folders

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Scan Jobs**.
3. Click **Add a Scan Job**.
   The **Scan Job Creation** window opens.
4. Enter a name for this task.
5. Select one of the following options.

Option	User Action
All folders	Click **All folders**.
Specific folders	**a.** Click **Specific folders**. **b.** Select a shared folder from the drop-down menu. **c.** Click **Add**. **Tip** To remove a shared folder, click .

6. Click **Next**.
   The **Schedule** screen appears.
7. Select a scan frequency option and configure the settings if required.
8. Click **Next**.
   The **File Filter** screen appears.

9. Select one of the following file filter options:

Option	Description
Scan all files	Scans all files on the NAS for viruses.
Quick scan (Only potentially dangerous file types listed below)	Only file types in the list are scanned for viruses. You can modify the list.

10. Optional: Exclude files and folders from the virus scan.
    a. Select **Exclude files or folders**.
    b. Specify the files, file types, and folders to exclude from the scan.
11. Click **Next**.
    The **Scan Options** screen appears.
12. Enter the maximum file size for the virus scan.
13. Optional: Select at least one of the following options.

Option	Description
Scan compressed files content	Scans compressed files. **Note** You can specify the maximum compressed file size that Antivirus will scan.
Deep scan for document files	Scans Microsoft Office, iWork, RTF, PDF, and HTML files.

14. Click **Next**.
    The **Action to take when infected files are found** screen appears.
15. Select an option on what to do with infected files.

Option	Description
Only report the virus	QTS only reports detected viruses and does not take any further action. The detections will appear in **Reports**.
Move infected files to quarantine	QTS quarantines the infected files. You cannot access these files from shared folders. You can review the virus scan report in **Reports** and delete or restore infected files in **Quarantine**.

Option	Description
Delete infected files automatically	QTS deletes the infected files. **Important** These files are permanently deleted.

16. Click **Finish**.
    The scan job appears in the **Job Name** list.

Managing scan jobs

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Scan Jobs**.
3. Locate a scan job you would like to modify.
4. Select one of the following options.

Option	User Action
Run now	Select . QTS starts the scan job.
Edit	a. Select . The **Details** window opens. b. Modify the settings. c. Click **OK**. QTS modifies the scan job's settings.
View last run log	a. Select . The **Last run log** window opens. b. Optional: Click the text box to modify the run log. c. Click **Close**.
Delete	a. Select . A confirmation message appears. b. Click **Yes**. QTS deletes the scan job.

Managing reported scan jobs

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Applications** > **Antivirus** > **Reports**.
3. Optional: Specify the log retention period.
   a. Go to **Number of days to keep the logs**.
   b. Enter the number of days.

      Tip
      Enter a number between 1 to 999.

   c. Click **Apply**.
4. Optional: Archive expired logs.
   a. Select **Archive logs after expiration**.
   b. Specify the archive folder.
   c. Click **Apply**.
5. Locate the scan job you want to manage.
6. Select one of the following options.

Option	User Action
Download	Select . QTS downloads the scan job as a text document to your computer. **Tip** To download all job logs, click **Download All Logs**.
Delete	a. Select . A confirmation message appears. b. Click **Yes**. QTS deletes the scan job.

Managing quarantined files

Warning
You cannot recover deleted quarantined files.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Quarantine**.
3. Locate the file or files you want to manage.

4. Perform one of the following options.

Option	User Action
Delete	Click  . QTS permanently deletes the selected file.
Delete Selected Files	a. Select files. b. Click **Delete Selected Files**. Only selected files in the list are permanently deleted.
Delete All Files	Click **Delete All Files**. All files in the list are permanently deleted.
Restore	Click  . QTS restores the file to its shared folder.
Restore Selected Files	a. Select files. b. Click **Restore Selected Files**. Only selected files in the list are restored to their shared folders.
Exclude List	Click  . QTS restores the file to its shared folder and adds the file to the exclude list.

Servers

Depending on your needs, you can configure the NAS to host websites, create VPN connections for secure data transmission, and more.

Web server

You can use the NAS to host websites and establish an interactive website.

Enabling the web server

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Web Server** > **Web Server**.
3. Select **Enable Web Server**.

4. Optional: Configure the Web Server settings.
   a. Specify a port number.

      Note
      The default port is 80.

   b. Select **Enable HTTP compression** to improve transfer speeds and bandwidth utilization. This setting is enabled by default.

      Warning
      Disabling this setting may increase security, but will increase bandwidth utilization.

5. Optional: Configure the secure connection (HTTPS) settings.
   a. Select **Enable secure connection (HTTPS)**.
   b. Select a TLS version. The default TLS version is 1.2.

      Warning
      Selecting the latest TLS version may decrease compatibility for other clients in your system.

   c. Select **Enable strong cipher suites**.
   d. Specify a port number.
   e. Optional: Select **Force secure connection (HTTPS) only** to require all users to connect to the device using only HTTPS.
6. Set the maximum client connection limit.
7. Optional: Select **Do not allow Web Server embedding in IFrames**.
8. Optional: Allow specific websites to embed Web Server in IFrames.
   a. Click **Allowed Websites**.
      The **Allowed Websites** window appears.
   b. Click **Add** to add a website to the list.
   c. The **Add Host Name** window appears.
   d. Specify a host name.
   e. Click **Add**.
      The host name is added to the allowed websites list.
   f. Optional: Select a website, and then click **Delete** to delete a website from the list.
   g. Click **Apply**.
9. Optional: Select **Enable X-Content-Type-Options HTTP header** to protect your device from attacks that exploit MIME sniffing vulnerabilities.

10. Optional: Select **Enable Content-Security-Policy-HTTP header** to protect your device from attacks that exploit Cross Site Scripting (XSS) and data injection vulnerabilities.
11. Click **Apply**.

    Tip
    To restore the default configuration settings at any time, click **Restore**.

    QTS enables the web server.

Modifying the PHP configuration

The default PHP settings are defined by the php.ini configuration file. You can modify this file to define settings such as execution time, memory limit, and maximum file upload size.

Important
To modify the PHP configuration, you must first enable the Web server. For details, see Web server.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Web Server** > **Web Server**.
3. Below **php.ini Maintenance**, perform one or more tasks.
4. Optional: Upload a php.ini file.
   a. Click **Upload**.
      The **Upload php.ini** window opens.
   b. Click **Browse**.
      The **Open** window opens.
   c. Select a php.ini file.
   d. Click **Upload**.

   QTS uploads the file.
5. Optional: Edit a php.ini file.
   a. Click **Edit**.
      The **Edit php.ini** window opens.
   b. Edit the php.ini file.
   c. Click **Apply**.

   QTS saves the changes.

6. Optional: Restore a php.ini file.

   a. Click **Restore**.
   A confirmation message appears.

   b. Click **OK**.

   QTS restores the default php.ini file.

Enabling and creating a virtual host

Virtual hosting allows you to use your NAS to host multiple websites.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Web Server** > **Virtual Host**.
3. Select **Enable Virtual Host**.
4. Click **Apply**.
   You can now create a virtual host.
5. Click **Create a Virtual Host**.
   The **Advanced Options** window opens.
6. Enter a host name.
7. Select a root directory.
8. Select a protocol.
9. Enter a port number.
10. Click **Apply**.
    The virtual host appears in the Host Name list.

LDAP server

Lightweight Directory Access Protocol (LDAP) is an open and cross-platform protocol used for accessing and managing a directory service. Enabling the LDAP server allows users to access and share your directory service.

> **Note**
> This feature is unavailable when there is no system volume.

Enabling the LDAP server

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **LDAP Server**.
3. Select **Enable LDAP Server**.
4. Enter a domain name.

5. Specify a password.
6. Verify the password.
7. Select a TLS version.
8. Optional: Click **Initialize**.

   Warning
   Initializing the LDAP database will delete all users and groups from the LDAP server.

9. Click **Apply**.

Backing up the LDAP database

Note
To back up the LDAP database, you must first enable the LDAP server.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **LDAP Server** > **Backup/Restore**.
3. Select **Back up Database**.
4. Configure the backup settings.
   a. Specify the backup frequency.
   b. Specify the start time.
   c. Select the destination location.
   d. Select the backup option.
      - **Overwrite existing backup file (LDAP_Backup.exp)**: Deletes the existing LDAP database backup file and creates a new backup file.
      - **Create a new file for each backup and append the date to the filename (LDAP_backup_yyyy_mm_dd.exp)**: Keeps the existing LDAP database backup file and creates a new backup file and includes the date of the backup to the filename.
5. Click **Apply**.

The system makes a backup immediately and will repeat this process according to the specified schedule.

Restoring an LDAP database

Note
To restore the LDAP database, you must first enable the LDAP server.

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Applications** > **LDAP Server** > **Backup/Restore**.
3. Under **Restore LDAP Database**, click **Browse**.
   The file explorer window opens.
4. Select the LDAP backup file.
5. Click **Open**.
   The file explorer window closes.
6. Click **Import**.
   The **Import LDAP Database** window appears.
7. Click **OK**.
8. Specify the administrator account password.
9. Click **Apply**.

QTS starts restoring the LDAP database.

MariaDB server

MariaDB is an open-source relational database management system compatible with MySQL. You can use MariaDB for hosting your website database on the NAS. QTS allows you to configure and migrate a MariaDB database to your NAS or to a server through the MariaDB 5 or MariaDB 10 app. The app is not pre-installed in QTS.

MariaDB server requirements

Software requirements	Description
Operating system	QTS 5.0.0 or later
App	MariaDB 5 or MariaDB 10 app Download and install the app version that meets your database requirements from App Center. For details, see Installing an app from App Center.

Configuring the MariaDB database

Important

- On devices with QTS 4.5.4 or earlier, if the SQL server is enabled during the firmware update, the system automatically downloads the MariaDB 5 app and migrates the SQL server data to MariaDB.
- You can install either the MariaDB 5 or MariaDB 10 app. If you install both app versions on your NAS, MariaDB 5 will be set as the default database server.

You can configure the MariaDB database using the following methods during setup:

Methods	Description
Creating a MariaDB database	Create a new MariaDB version 5 or Maria DB version 10 database by configuring the TCP/IP network configurations and database password. For details, see Creating a MariaDB database.
Restoring a MariaDB Database	Restore an existing MariaDB version 5 or MariaDB version 10 database by configuring the TCP/IP network configurations. For details, see Restoring a MariaDB database.
Migrating a MariaDB 5 Database to MariaDB 10	If the MariaDB 10 app is installed on your NAS, you can migrate an existing MariaDB version 5 database to a MariaDB version 10 database. For details, see Migrating a MariaDB 5 database to MariaDB 10.

Creating a MariaDB database

Warning
Creating a new MariaDB database will overwrite an existing MariaDB database.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **MariaDB**.
   The **MariaDB Setup Wizard** window opens.

   Note
   The MariaDB setup wizard only appears during app initialization. To configure more advanced database features and settings, use the php.ini maintenance file.

3. Click **Start**.
   The **Database Actions** screen appears.
4. Select **Create a new database**.
5. Click **Next**.
   The **Default Instance Properties** screen appears.
6. Specify a root password.

   Important
   - The password must contain 8 to 64 bytes of UTF-8 characters.
   - The password cannot be "admin" or blank.
   - If the system detects a weak password, the MariaDB server will be automatically disabled until a stronger password is configured.

7. Confirm the password.
8. Optional: Enable TCP/IP networking.
   a. Select **Enable TCP/IP networking**.
   b. Specify the port number.

      Tip

      - MariaDB 5: The default port number is 3306.
      - MariaDB 10: The default port number is 3307.

9. Click **Apply**.
   QTS creates the MariaDB database. The **Finish** screen appears.

   Note
   It may take a few minutes for the system to set up the database.

10. Click **Finish**.
    QTS enables the MariaDB server.

Restoring a MariaDB database

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **MariaDB**.
   The **MariaDB Setup Wizard** window opens.

   Note
   The MariaDB setup wizard only appears during app initialization. To configure more advanced database features and settings, use the php.ini maintenance file.

3. Click **Start**.
   The **Database Actions** screen appears.
4. Select **Restore an existing database**.
5. Click **Next**.
   The **Default Instance Properties** screen appears.
6. Optional: Configure TCP/IP networking.
   a. Select **Enable TCP/IP networking**.

      Note
      This option is enabled by default.

b. Specify the port number for TCP/IP networking.

> **Note**
> The default port is 3307.

7. Click **Apply**.
   QTS restores the MariaDB database. The **Finish** screen appears.

> **Note**
> It may take a few minutes for the system to restore the database.

8. Click **Finish**.
   QTS enables the MariaDB server.

Migrating a MariaDB 5 database to MariaDB 10

This feature is only available in the MariaDB 10 app.

1. Log on to QTS as administrator.
2. Install the MariaDB 10 app.

> **Note**
> For details, see Installing an app from App Center.

3. Open the MariaDB 10 app.
   The **MariaDB Setup Wizard** window opens.

> **Note**
> The MariaDB setup wizard only appears during app initialization. To configure more advanced database features and settings, edit the php.ini maintenance file. For details, see Modifying the PHP configuration.

4. Click **Start**.
   The **Database Actions** screen appears.
5. Select **Migrate a MariaDB 5 to a MariaDB 10 database**.
6. Click **Next**.
   The **Default Instance Properties** screen appears.
7. Optional: Configure TCP/IP networking.

a. Select **Enable TCP/IP networking**.

> **Note**
> This option is enabled by default.

b. Specify the TCP/IP networking port.

> **Note**
> The default port is 3307.

8. Click **Apply**.
   QTS migrates the existing MariaDB 5 database to MariaDB 10. The **Finish** screen appears.

> **Note**
> The data migration may take a few minutes to complete.

9. Click **Finish**.
   QTS enables the MariaDB server.

Enabling or disabling the MariaDB server

> **Important**
> On devices with QTS 4.5.4 or earlier, if the SQL server is enabled during the firmware update, the system automatically downloads the MariaDB 5 app and migrates the SQL server data to MariaDB.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **MariaDB**.
   The MariaDB application opens.
3. Perform one of the following operations.
   - Click  to enable the MariaDB server.
   - Click  to disable the MariaDB server.

Managing the MariaDB account and database

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **MariaDB**.
   The MariaDB application opens.
3. Click **Account and Database**.
4. Perform any of the following tasks.
5. Reset the root password of the MariaDB database.

> **Warning**
> Resetting the root password will restart the MariaDB database.

Important
To protect your device, the system will automatically detect weak MariaDB server root passwords and require you to change the password. Follow the on-screen instructions to change the root password.

a. Click **Reset**.
The **Reset Root Password** screen appears.

b. Specify a new password.

Note
- The password must contain 8 to 64 bytes of UTF-8 characters.
- The password cannot be "admin" or blank.

c. Confirm the password.

d. Click **Next**.

e. Click **Yes**.

f. The root password is changed.

6. Reset the user password of the MariaDB account.

a. Click **Reset**.
The **Reset User Passwords** screen appears.

b. Enter the root password.

c. Click **Next**.

d. Select a user account.

e. Specify a new password.

Note
- The password must contain 8 to 64 bytes of UTF-8 characters.
- The password cannot be "admin" or blank.

f. Confirm the password.

g. Click **Apply**.

7. Reinitialize the MariaDB database.

Warning
Reinitializing the database will delete all data in the database.

a. Click **Reinitialize**.
   A confirmation message appears.

b. Click **Yes**.
   The **MariaDB Setup Wizard** screen appears.

Modifying the TCP/IP network settings

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **MariaDB**.
   The MariaDB app opens.
3. Click **Information**.
4. Select **Enable TCP/IP networking**.
5. Specify a port number.

   Note

   - MariaDB 5: The default port number is 3306.
   - MariaDB 10: The default port number is 3307.

6. Click **Apply**.
   The TCP/IP networking settings are updated.

Syslog server

You can configure the NAS as a syslog server. This allows you to collect log messages from different devices in one location.

Enabling the syslog server

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Syslog Server** > **Server Settings**.
3. Select **Enable Syslog Server**.
4. Optional: Enable the TCP protocol on the server.
   a. Select **Enable TCP**.
   b. Enter a TCP port number.
5. Optional: Enable the UDP protocol on the server.
   a. Select **Enable UDP**.
   b. Enter a UDP port number.

6. Optional: Configure the log settings.
   a. Specify the maximum log size.

      Tip
      The log size range is 1 to 100.

   b. Select the log destination folder.
   c. Enter the log file name.
7. Optional: Enable the email notification settings.

   Note
   The NAS sends an email to up to 2 email addresses when the severity of the received syslog message matches the specified level.

   a. Select **Enable the email notification**.
   b. Select a severity level.

Level	Severity	Description
0	**Emerg**	The system is unusable.
1	**Alert**	The system requires immediate attention.
2	**Crit**	The system has critical conditions.
3	**Err**	The system has error conditions.
4	**Warning**	The system has warning conditions.

   c. Click **Configure Notification Rule**.
   The **Create event notification rule** window opens.

Adding a Syslog server filter

This task allows the NAS to only receive syslog messages that match a specified filter.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Syslog Server** > **Filter Settings**.
3. Click **Add a Filter**.
   The **Add a Filter** window opens.

4. Configure the filter.
   a. Select the filter type.
      - **Facility**
      - **Severity**
      - **Hostname**
      - **Application**
      - **Message**
      - **IP**
   b. Select a filter option.
      - **greater than or equal to**
      - **less than or equal to**
      - **equals**
      - **starts with**
      - **contains**
      - **not equals**
      - **does not start with**
      - **does not contain**
   c. Enter the filter condition.
   d. Click **Add**.

      Tip
      To remove an existing filter, click **Remove**.

5. Optional: Manually configure a filter.
   a. Select **Manual Edit**.
   b. Type the filter conditions.
6. Click **Apply**.
   QTS adds the syslog filter.

Managing syslog filters

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **Syslog Server** > **Filter Settings**.
3. Locate the filter you want to modify.

4. Click to enable the filter.
   QTS enables the syslog filter.
5. Click to disable the filter.
   QTS disables the syslog filter.
6. Modify the syslog filter.
   a. Click .
      The **Filter** window opens.
   b. Modify the filter.
   c. Click **Apply**.

   QTS saves the filter information.
7. Delete the syslog filter.
   a. Select one or more filters.
   b. Click **Delete**.
      A confirmation message appears.
   c. Click **Yes**.

   QTS deletes the selected filters.

RADIUS server

You can configure the NAS to become a remote authentication dial-in user service (RADIUS) server. The RADIUS server provides centralized authentication, authorization, and account management for computers to connect and use as a network service.

Enabling the RADIUS server

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **RADIUS Server** > **Server Settings**.
3. Select **Enable RADIUS Server**.
4. Optional: Select **Grant dial-in access to system user accounts**.

   Note
   This option allows local NAS users to access network services using the login credentials for RADIUS clients.
5. Click **Apply**.

Creating a RADIUS client

A RADIUS client is a client device, client program, or a client software utility. You can create up to 10 clients.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **RADIUS Server** > **RADIUS Clients**.
3. Click **Create a Client**.
   The **Create a Client** window opens.
4. Enter the following information.
   - **Name**
   - **IP Address**
   - **Prefix Length**
   - **Secret Key**
5. Click **Apply**.
   QTS creates the RADIUS client.

Managing RADIUS clients

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **RADIUS Server** > **RADIUS Clients**.
3. Locate the client you want to modify.
4. Click to enable the client.
   QTS enables the client.
5. Click to disable the client.
   QTS disables the client.
6. Edit the client information.
   a. Click .
      The **Edit Client** window opens.
   b. Configure the client information.
   c. Click **Apply**.

   QTS saves the client information.
7. Delete the client information.
   a. Select one or more clients.
   b. Click **Delete**.
      A confirmation message appears.
   c. Click **Yes**.

   QTS deletes the selected clients.

Creating a RADIUS user

A RADIUS user is the account used for RADIUS authentication. You can create as many users as the NAS supports.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **RADIUS Server** > **RADIUS Users**.
3. Click **Create a User**.
   The **Create a User** window opens.
4. Enter the following information.
   - **Name**
   - **Password**
   - **Verify Password**
5. Click **Apply**.
   QTS creates the RADIUS user.

Managing RADIUS users

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **RADIUS Server** > **RADIUS Users**.
3. Locate a RADIUS user you want to modify.
4. Click to enable the user.
   QTS enables the user.
5. Click to disable the user.
   QTS disables the user.
6. Change the RADIUS user password.
   a. Click .
      The **Edit User** window opens.
   b. Modify the settings.
   c. Click **Apply**.

   QTS saves the new password.
7. Delete RADIUS users.
   a. Select one or more users.

b. Click **Delete**.
A confirmation message appears.

c. Click **Yes**.

QTS deletes the selected users.

Enabling the TFTP server

Enabling the Trivial File Transfer Protocol (TFTP) Server allows you to configure network devices and boot computers on a remote network for system imaging or recovery. TFTP does not provide user authentication and you cannot connect to it using a standard FTP client.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Applications** > **TFTP Server**.
3. Select **Enable TFTP Server**.
4. Specify a UDP port.

   Note
   The default UDP port is 69. Change this port only if necessary.

5. Specify the root directory.
6. Optional: Enable TFTP logging.

   Note
   This option saves the TFTP logs as files. QNAP recommends viewing the log files using Microsoft Excel or WordPad on Windows, or TextEdit on macOS.

   a. Select **Enable TFTP logging**.
   b. Specify the folder for saving log files.
   c. Specify the access right.

7. Configure TFTP access.
   - **Anywhere**: Allows TFTP access from any IP address.
   - **Certain IP range only**: Allows TFTP access from IP addresses in the specified IP range only. Enter the start and end IP addresses of the IP range.
8. Click **Apply**.
   QTS enables the TFTP server.

Enabling the NTP server

The NTP server allows other network devices to synchronize their time with the NAS.

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Applications** > **NTP Server**.
3. Select **Enable NTP Server (NTP server is Ready)**.
4. Optional: Select at least one operating mode.

Operating Mode	Description
Broadcast	Allows the NTP server to periodically send broadcast packets with the IP address 255.255.255.255. You can use this to synchronize your time.
Multicast	Allows the NTP server to periodically send multicast packets. Enter a multicast IP after selecting this option.
Manycast	Allows the NTP server to listen for manycast requests from NTP clients and reply to received client requests. Enter a multicast IP after selecting this option.

5. Click **Apply**.
   QTS enables the NTP server.

6. File Station

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

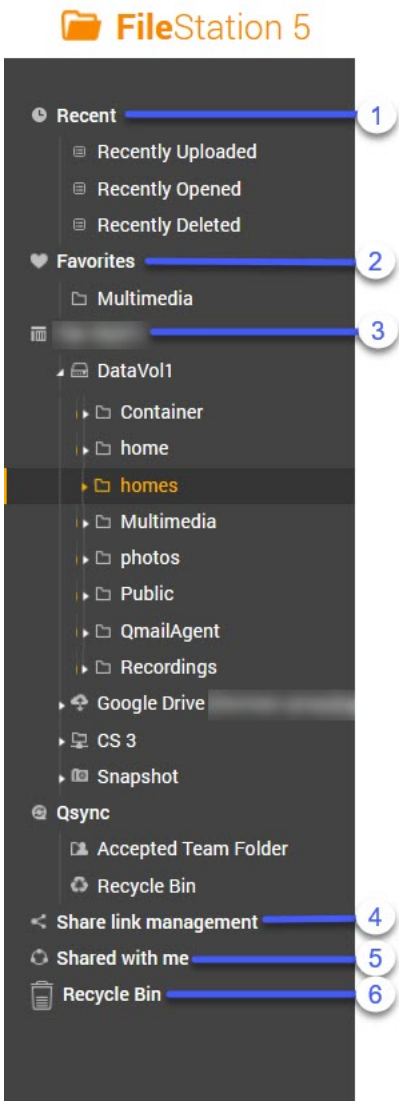
Category	Detail
Web browser	• Microsoft Edge • Mozilla Firefox 3.6 or later • Apple Safari 5 or later • Google Chrome
Java program	Java Runtime Environment (JRE) 7 or later
Flash player	Adobe Flash Player 9 or later is required for viewing media files.

File Station user interface

You can perform file and folder actions from the toolbar and the left panel.

Label	Item	Description
1	Search	Search files and folders by their name or type. **Tip** You can search files in a folder by clicking the folder. The folder name is displayed in the search box.
3	Background Task	Open the background tasks of your mount, folder, or file operations.

Label	Item	Description
4	Network Media Player	Stream videos, photos, and music to compatible devices on your network.
4	Refresh	Refresh the current page.
5	Smart Filter	Filter files and folders based on the specified criteria.
6	More Settings	Configure File Station settings, open the Help guide, or view application information.
7	Remote Mount	Manage files across local, external, remote, and cloud storage resources on a single interface. To use this feature, install HybridMount from App Center. For more information on HybridMount, go to the QNAP website.
8	Browsing Mode	Select a browsing mode.
9	Create folder	Create a folder, shared folder, snapshot shared folder, or share a space with another NAS user.
10	Copy	Copy the selected files and folders. **Note** This button only appears when a file or folder is selected.
11	Upload	Upload files or folders to the selected shared folder.
12	More Actions	Perform different tasks. **Note** Some task options only appear when you select certain types of files.
13	Share	Share the selected files and folders. **Note** This button only appears when a file or folder is selected.
14	Snapshot	Open Snapshot Manager or view the Snapshot Manager quick tutorial.



Label	UI Element	Description
1	Recent	Displays recenty uploaded, opened, or deleted files.
3	Favorites	Displays bookmarked folders.
2	Volume	Displays all the folders on the volume, including shared folders. Default shared folders vary depending on the NAS model.
4	Share link management	Displays links to NAS files shared by the current user account. **Note** Users in the administrator group can see links shared by all NAS users.
5	Shared with me	Displays files and folders shared with the current user account.

Label	UI Element	Description
6	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.
Qsync	Displays files, folders, and team folders from Qsync.
SMB shared folder	Displays files and folders from a shared folder mounted through SMB protocol. **Note** To view the folder name, connection name, and the file protocol, hover your cursor over an SMB shared folder.
NFS shared folder	Displays files and folders from a shared folder mounted through NFS protocol. **Note** To view the folder name, connection name, and the file protocol, hover your cursor over an NFS shared folder.
File Cloud Gateway shared folder	Displays files and folders from a shared folder mounted through a File Cloud Gateway connection via HybridMount.

Depending on your setup, the following mounts created in HybridMount may also appear on the list.

Mount	Description
CIFS/SMB	Displays a list of connections mounted through CIFS/SMB protocol.
NFS	Displays a list of connections mounted through NFS protocol.
FTP	Displays a list of connections mounted through FTP protocol.
WevDAV	Displays a list of connections mounted through a local network or over the internet.

Mount	Description
Cloud services	Displays a list of connections mounted through a cloud service. **Note** To view the folder name, connection name, and the cloud provider, hover your cursor over the cloud mount.

You can perform the following tasks for a volume on the left panel.

Tip
To see the task options, hover the cursor over a volume and then click  .

Left Panel Tasks

Task	Description
Create a shared folder	Click to create 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.

Depending on your NAS model and environment, the following icons may appear beside each available volume.

Volume Icons

Icon	Name	Description
	On Demand Tiering	This icon appears when auto-tiering is enabled on the volume.
	Snapshots	This icon appears when snapshots are available for the volume. For details, go to the Snapshot section of the QTS User Guide.
	Cache Acceleration	This icon appears when acceleration is enabled on the volume.
	Volume Encryption	This icon appears when the volume is encrypted.
	Volume Synchroni-zation	This icon appears when the cloud volume is synchronizing data.

Supported file formats

Category	File Extension
Image	• BMP • JPG • JPE • PNG • TGA • GIF • HEIC • HEIF • WebP **Note** The availability of multimedia file formats may vary depending on the multimedia services enabled on the NAS.
Music	• MP3 • FLAC • OGG • WAV • AIF • AIFF **Note** The availability of multimedia file formats may vary depending on the multimedia services enabled on the NAS.

Category	File Extension
Video	• AVI • MP4 • WebM **Note** The availability of multimedia file formats may vary depending on the multimedia services enabled on the NAS.
Microsoft Office (Word, Excel, PowerPoint)	• DOC • DOCX • PPT • PPTX
Others	• TXT • PDF

File and folder operations

File Station enables you to perform the following tasks.

Operation	File Tasks	Folder Tasks
Store	• Uploading files and folders	
Access	• Downloading files and folders • Viewing file or folder properties • Modifying file or folder permissions	

Operation	File Tasks	Folder Tasks
Access	• 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 • Opening image files using Image2PDF	• Viewing storage information • Viewing Qsync folders • Managing share links • Viewing files and folders shared with me
Organize	• Sorting files and folders • Copying files and folders • Moving files and folders • Renaming files or folders • Compressing files and folders • Extracting compressed files or folders	
	• Deleting a file • Restoring a deleted file • Encrypting files • Decrypting files • Mounting an ISO file • Unmounting an ISO file	• Creating a folder • Creating a desktop shortcut • Adding a folder to Favorites • Removing a folder from Favorites
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	

Operation	File Tasks	Folder Tasks
Share	-	• Creating a shared folder • Creating a snapshot shared folder • Sharing space with a new user • Locking or unlocking an encrypted shared folder
Play	• Playing an audio file • Playing a video file • Playing a video file using CAYIN MediaSign Player • Opening a 360-degree image or video file • Streaming to a Network Media Player	-
Transcode	• Adding a file or folder to the transcoding folder • Canceling or deleting transcoding	
	Viewing transcode information	-
Others	Keeping a folder or a file in reserved cache	
	Converting Apple iWork files to Microsoft Office files	Removing a folder from reserved cache

Uploading files and folders

You can upload files or folders either individually or in batches.

1. Open File Station.
2. Open the destination folder.
3. Drag and drop files and folders from your computer to the destination folder.

   Tip

   You can upload files or folders separately. Click  and select **File** or **Folder**. Select the files or folders you want to upload and then click **Open** or **Upload**. Uploading folders this way requires the Google Chrome web browser.

   The **Background Task** window opens.

4. 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 you configure the settings. You can still change the policy in **File Station** > **More Settings** > **Settings** > **File Transfer**.

5. Click **OK**.
File Station uploads the selected items.

Downloading files and folders

You can download files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Click **Download**.
Using the left panel	**a.** Right-click a folder. **b.** Click **Download**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Click **Download**.

File Station downloads the items to your computer.

Viewing file or folder properties

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Properties**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Properties**. **Tip** If the folder you want to view appears on the left panel, you can right-click the folder from the left panel and select **Properties**.

Depending on your selected items, the **Properties** window opens and displays the following information.

Field	Description
Selected items	Displays how many items are selected.
Type	Displays the folder or file type.
Size	Displays the file or folder size. **Tip** If you selected multiple items, click  to display the total size and file count.
Location	Displays the file or folder location.
Modified Date	Displays the date the file or folder was last modified.
Storage Pool	Displays the name of the storage pool on which the folder is stored.

Field	Description
Volume	Displays the name of the volume on which the folder is stored.

4. Click **Close**.

Modifying file or folder permissions

To configure more advanced permission settings for individual users, you need to enable advanced folder permissions in **Control Panel** > **Privilege** > **Shared Folders** > **Advanced Permissions**.

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file or folder. **b.** Click  . **c.** Select **Properties**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Properties**.

The **Properties** window opens.

4. Click **Permission**.
5. Enable or disable the following permissions for the owner, group, or other users on the list.

Basic Settings

Permission	Description
Read	Allows a user to view the file or folder.
Write	Allows a user to make changes to the file or folder.
Execute	Allows a user to run a file.

Note
You can only configure file or folder permissions for owners, groups, and other accounts under basic settings.

Advanced Settings

Permission	Description
Read Only	Allows a user to view the file or folder.
Read/Write	Allows a user to view and make changes to the file or folder.
Deny	Denies any access to the file or folder.

Tip
You can click **+** to add users to the list and click **-** to remove users from the list.

6. Optional: Select the access rights for guest users.
7. Optional: Specify the ownership of the file or folder.
   a. Click .
   b. Select a user.
   c. Click **Set**.
8. Optional: Enable one or more of the following settings.
   - 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 of this folder, files, and subfolders
9. Click **Apply**.

Opening a file

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the file. b. Click . c. Select **Open**.

Method	Steps
Using the context menu	Right-click and then select **Open**.

Open the file directly	Double-click the file.
	Note
	• File Station performs various actions depending on the type of the selected file.
	• For document files, you can choose an action from the following options.
	  • **Edit with Office Online**
	  • **View in Google Docs**
	  • **Open with Chrome Extension**
	  • **Open with web browser**
	• Opening certain files may require a particular app to be installed from App Center or a particular software license to be activated.

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
Using the toolbar	a. Select the file. b. Click  . c. Select **Open with Chrome Extension**.

Method	Steps
Using 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
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Open with Text Editor**.
Using 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.

You can open and view files in Google Docs. To use this feature, your web browser must allow pop-up windows.

1. Open File Station.
2. Locate the file.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the file. b. Click  . c. Select **View in Google docs**.
Using the context menu	Right-click and then select **View in Google docs**.

File Station opens a preview of the file in Google Docs.

Viewing a file in Microsoft Office Online

This task requires that you enable myQNAPcloud Link.

You can open and edit Microsoft Word, Excel, and Powerpoint files using Office Online. To use this feature, your web browser must allow pop-up windows.

> **Note**
> Editing a file in Microsoft Office Online overwrites the file saved on the NAS.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the file. b. Click  . c. Select **Edit with Office Online**.
Using the context menu	Right-click the file and then select **Edit with Office Online**.

File Station opens the file in Microsoft Office Online.

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.

Viewing storage information

1. Open File Station.
2. Locate the NAS name in the left panel.
3. Click  .
4. Click **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.

5. Click **Close**.

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

Share link management allows you to view, manage, and share previously created shared links easily and quickly.

1. Open File Station.
2. On the left panel, click **Share link management**.
   File Station displays the list of shared files and folders.

   Note

   - File Station automatically checks and deletes expired links.
   - You can share a maximum number of 100,000 shared files and folders. If each link shares one file or folder, you can create 100,000 share links. However, if each link shares 500 files or folders, you can only create 200 share links.

3. Select an item from the list and then perform one of the following tasks.

Task	User Action
Re-share	Click and then select one of the following share methods. • Share By Email. • Share on a social network • Use share links • Share 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.

Sorting files and folders

Sort files and folders to make them easier to see and find.

1. Open File Station.
2. Click .
3. Select one the following.
   - List
   - Large icons
   - Medium icons
   - Small icons

   File Station displays files and folders according to the selected option.
4. Click a column title.

   Note
   This option is only available in the list view.

   File Station sorts files in an ascending or descending order based on the selected column.

Copying files and folders

You can copy files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Click . b. Select **Copy to / Move to** and then select **Copy to**. The **Folder Selector** window opens. c. Select the destination folder. d. Select a mode. e. Optional: Select **Merge selected file transfer tasks**. f. Click **Apply**.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Go to the destination folder. **c.** Click  .
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Copy**. **c.** Go to the destination folder. **d.** Right-click inside the folder and then select **Paste**. **Note** You can aslo right-click a folder from the left panel and select **Paste**.
Using 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 duplicate files** • **Copy and overwrite duplicate files** • **Copy and rename duplicate files**
Using keyboard shortcuts	**a.** Press **CTRL + C** or **Command-C**. **b.** Go to the destination folder. **c.** Press **CTRL + V** or **Command-V**.
Using the left panel **Note** This option applies to subfolders.	**a.** Right-click a subfolder. **b.** Hover your mouse over **Copy to/ Move to**, and then select **Copy to**. The **Folder Selector** window opens. **c.** Select a destination folder. **d.** Optional: Select a mode. **e.** Optional: Select **Merge selected file transfer tasks**.

Method	Steps
Using the left panel **Note** This action applies to mounts.	**a.** Right-click a mount. **b.** Select **Copy:/MOUNTNAME**. **c.** Go to the destination folder. **d.** Click  .

File Station creates a copy of the selected items.

Moving files and folders

You can only move subfolders underneath a mount. You can move files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Copy to / Move to** and then select **Move to**. The **Folder Selector** window opens. **c.** Select the destination folder. **d.** Specify a mode. **e.** Optional: Select **Merge selected file transfer tasks**. **f.** Click **Apply**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Right-click the file and then select **Copy to/Move to** and **Move to**. The **Folder Selector** window opens. **c.** Select the destination folder. **d.** Select a mode. **e.** Optional: Select **Merge selected transfer tasks**. **f.** Click **Apply**.

Method	Steps
Using the context menu	**a.** Right-click a selected file or folder and then select **Cut**. **b.** Select the destination folder. **c.** Right-click inside the folder and then select **Paste**.
Using the left panel	**a.** Right-click a subfolder. **b.** Hover your mouse over **Copy to/ Move to**, and then select **Move to**. The **Folder Selector** window opens. **c.** Select a destination folder. **d.** Optional: Select a mode. **e.** Optional: Select **Merge selected file transfer tasks**. **f.** Click **Apply**.

File Station moves the selected items to the specified folder.

Renaming files or folders

You can only rename one file or folder at a time.

1. Open File Station.
2. Locate and select the file or folder.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Rename**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Rename**.

The **Rename** window opens.

4. Specify a new name for the file or folder.
5. Click **OK**.
File Station renames the file or folder.

Compressing files and folders

1. Open File Station.

2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Compress(Zip)**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Compress(Zip)**.

The **Compress** window opens.

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** • **Update and add files** • **Update existing files** • **Synchronize files**

5. Optional: Specify a password to encrypt the file.
6. Click **OK**.
File Station compresses the selected items and creates an 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
Using the toolbar	a. Select the file. b. Click  . c. Select **Extract**.
Using the context menu	a. Right-click the file. b. Select **Extract**.

4. Select one of the following file extraction options.

Option	Description
Extract files	Select specific files to extract.
Extract here	Extracts 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.

Deleting a file

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the file. b. Click  . c. Select **Delete**.

Method	Steps
Using 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

This task requires that you enable Recycle Bin for the shared folders.

1. Open File Station.
2. Go to **Recycle Bin**.
3. Locate the file.
4. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Recover**.
Using the context menu	**a.** Right-click the file. **b.** Select **Recover**.

A confirmation message appears.

5. Click **Yes**.
   File Station restores the selected file.

Encrypting files

1. Open File Station.
2. Locate and select one or more files.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Click  . b. Select **Encrypt**. The **Encrypt** window opens. c. Specify a password. d. Verify the password. e. Select a mode. f. Select whether to encrypt and replace the original file. g. Click **OK**.
Using the context menu	a. Locate a file in the list and then right-click. b. Select **Encrypt**. The **Encrypt** window opens. c. Specify a password. d. Verify the password. e. Select a mode. f. Select whether to encrypt and replace the original file. g. Click **OK**.

Decrypting files

This task decrypts files directly in File Station. You can also use the QENC Decrypter to decrypt files. To download the QENC Decrypter, visit https://www.qnap.com/en/utilities/enterprise.

1. Open File Station.
2. Locate and select an encrypted file.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Click  . b. Select **Decryption**. The **Decryption** window opens. c. Specify the password. d. Select a mode. e. Click **OK**.
Using the context menu	a. Right-click the encrypted file. b. Select **Decryption**. c. Specify the password. d. Select a mode. e. Click **OK**.

Mounting an ISO file

1. Open File Station.
2. Upload an ISO file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the file. b. Click  . c. Select **Mount ISO**.
Using 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**.

Creating a folder

1. Open File Station.
2. Locate the destination folder.
3. Perform one of the following tasks.

Task	Steps
Using the toolbar	**a.** Click  **b.** Select **Folder**. The **Create folder** window opens. **c.** Specify the folder name. **d.** Click **OK**.
Using 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.

Creating a desktop shortcut

1. Open File Station.
2. Locate the folder.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the folder. **b.** Click  . **c.** Select **Create Shortcut to Desktop**.
Using 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
Using the toolbar	**a.** Select the folder. **b.** Click  . **c.** Select **Add to Favorites**.
Using 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
Using the toolbar	**a.** Select the folder. **b.** Click . **c.** Select **Remove from Favorites**.
Using 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.

Sharing a file or folder by email

Before starting this task, you must configure the QTS email settings in **Desktop** > > **E-mail Account**.

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	User Action
Using the toolbar	**a.** Select the file or folder. **b.** Click . **c.** Select **Via Email**.

Method	User Action
Using 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	User Action
Send from	Select the email delivery method. • Use NAS to mail the links. • Use local computer to mail the links.
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 line.
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Enter a name for the link or use the current name of the file or folder. **Note** A link name cannot contain the following characters: / | \ : ? < > * "

Field	User Action
Domain name/IP	Select the domain name or IP address. **Tip** The following domains and IP addresses are supported: • **myQNAPcloud**: Provides a link to the shared file or folder using the DDNS address set in myQNAPcloud. • **WAN**: Provides a link to the shared file or folder to other computers using a different network. • **LAN**: Provides a link to the shared file or folder to other computers using the same local network. • **SmartShare**: Provides a SmartURL via myQNAPcloud Link to the shared file or folder. • **All available links**: Provides links to the shared file or folder using all of the available domains and IPs. **Note** The recipients get direct read access.
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 sharing files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
Allow file upload to this folder	Allow users to upload files to this folder. **Note** This setting only appears when sharing folders.

Field	User Action
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** To include the password in the email, select **Show the password in the email**.

6. Click **Share Now**.
   File Station sends an email to the recipient.

Sharing a file or folder on a social network

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	User Action
Using the toolbar	a. Select the file or folder. b. Click  . c. Select **To Social Network**.
Using the context menu	a. Right-click the file or folder. b. Select **Share** and then select **To Social Network**.

   The **Share** window appears.

4. Configure the following settings.

Field	User Action
Social Network	Select the social network website.

Field	User Action
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Enter a name for the link or use the current name of the file or folder. **Note** A link name cannot contain the following characters: / | \ : ? < > * "
Domain name/IP	Select the domain name or IP address. **Tip** The following domains and IP addresses are supported: • **myQNAPcloud**: Provides a link to the shared file or folder using the DDNS address set in myQNAPcloud. • **WAN**: Provides a link to the shared file or folder to other computers using a different network. • **LAN**: Provides a link to the shared file or folder to other computers using the same local network. • **SmartShare**: Provides a SmartURL via myQNAPcloud Link to the shared file or folder. • **All available links**: Provides links to the shared file or folder using all of the available domains and IPs. **Note** The recipients get direct read access.
Show SSL in URL	Use an HTTPS URL.

Field	User Action
On-the-fly transcoding	Allow users to transcode videos on the fly. **Note** • This setting only appears when sharing files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
Allow file upload to this folder	Allow users to upload files to this folder. **Note** This setting only appears when sharing folders.
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

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	User Action
Using the toolbar	a. Select the file or folder. b. Click  . c. Select **Create share link only**.

Method	User Action
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** and then select **Create share link only**.

The **Share** window appears.

Note
Up to 100,000 files and folders, including subfolders of shared folders, can be shared via share links at any one time.

4. Configure the following settings.

Field	User Action
Link Name	Enter a name for the link or use the current name of the file or folder. **Note** A link name cannot contain the following characters: / | \ : ? < > * "
Domain name/IP	Select the domain name or IP address. **Tip** The following domains and IP addresses are supported: • **myQNAPcloud**: Provides a link to the shared file or folder using the DDNS address set in myQNAPcloud. • **WAN**: Provides a link to the shared file or folder to other computers using a different network. • **LAN**: Provides a link to the shared file or folder to other computers using the same local network. • **SmartShare**: Provides a SmartURL via myQNAPcloud Link to the shared file or folder. • **All available links**: Provides links to the shared file or folder using all of the available domains and IPs. **Note** The recipients get direct read access.

Field	User Action
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 sharing files. • To use on-the-fly transcoding, you must install and enable CAYIN MediaSign Player from App Center and activate a CAYIN MediaSign Player license.
Allow file upload to this folder	Allow users to upload files to this folder. **Note** This setting only appears when sharing folders.
Expire in	Specify the expiration date. **Note** This setting only appears when you share a folder.
Password	Require a password to access the link.

5. Click **Create Now**.
   File Station generates a link.

Sharing a file or folder with a NAS user

1. Open File Station.
2. Locate the file or folder.
3. Perform one of the following methods.

Method	User Action
Using the toolbar	a. Select the file or folder. b. Click  . c. Select **To NAS user**.

Method	User Action
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** and then select **To NAS user**.

The **Share** window appears.

4. Select the user to share the file or folder with.

Option	User Action
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 for each user in **Control Panel** > **Privilege** > **Users**.
New user	Create a new user account.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Enter a name for the link or use the current name of the file or folder. **Note** A link name cannot contain the following characters: / | \ : ? < > * "

Field	User Action
Domain name/IP	Select the domain name or IP address. **Tip** The following domains and IP addresses are supported: • **myQNAPcloud**: Provides a link to the shared file or folder using the DDNS address set in myQNAPcloud. • **WAN**: Provides a link to the shared file or folder to other computers using a different network. • **LAN**: Provides a link to the shared file or folder to other computers using the same local network. • **SmartShare**: Provides a SmartURL via myQNAPcloud Link to the shared file or folder. • **All available links**: Provides links to the shared file or folder using all of the available domains and IPs. **Note** The recipients get direct read access.
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 sharing files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
Allow file upload to this folder	Allow users to upload files to this folder. **Note** This setting only appears when sharing folders.

Field	User Action
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** • If you enable this option, this field cannot be empty. • To include the password in the email, select **Show the password in the email**.

6. Click **Share Now**.
   File Station shares the file with the specified user.

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 or end with a space • 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.

Field	Description
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 path automatically**: Creates a new root folder on the selected volume using the specified shared folder name. • **Enter path manually**: Select an existing folder as the root folder.

5. Optional: Enable folder encryption.

   a. Under **Folder Encryption**, select **Encryption**.
   Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.

   b. 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. **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, all data will become inaccessible.

6. Click **Next**.

7. Optional: Specify the access permissions for users.
   For details, see Shared folder permissions.

8. Click **Next**.
9. Optional: Configure properties.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
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	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is 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. **Important** • If space in the folder is insufficient when starting a new Time Machine backup, QTS automatically deletes the oldest Time Machine backup in the folder to free up space. • You should disable **Enable Network Recycle Bin** when **Set this folder as the Time Machine backup folder (macOS)** is selected to prevent automatically deleted Time Machine backups from filling the recycle bin.
Instant sync to disks when requested by SMB clients	Enabling this option allows the system to immediately synchronize data to disks when requested by SMB clients and therefore provides better data integrity. Disabling this option improves I/O performance but may increase the risk of data loss or corruption in the event of power outage or system failure.

10. Click **Finish**.

Tip
Hovering your mouse underneath the columns **Size**, **Folders**, and **Files** displays the shared folder's size, number of folders, number of files, and last update time.

Creating a snapshot shared folder

1. Open File Station.
2. On the menu bar, click  .
3. Select **Snapshot shared folder**.
   The **Create a Snapshot 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 or end with a space • 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. Click **Next**.
6. Optional: Configure user access permissions.
   a. Specify access permissions for each user.
7. Click **Next**.
8. Optional: Configure properties.
   a. Configure the following settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.

Option	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.
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.

9. Click **Finish**
   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.

Locking or unlocking an encrypted shared folder

After creating an encrypted shared folder, you can lock or unlock this folder to control user access.

1. Open File Station.

2. Locate an encrypted folder on the left panel.

Tip

File Station displays the following icons beside an encrypted shared folder.

Icon	Status
	The encrypted folder is locked.
	The encrypted folder is unlocked.

3. Perform one of the following tasks.

Tasks	Steps
Lock the shared folder	**a.** Right-click the shared folder. **b.** Select **Lock**.
Unlock the shared folder	**a.** Click the shared folder. A confirmation message appears. **b.** Click **Unlock**. **c.** Specify the password. **d.** Click **OK**.

Playing an audio file

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Play**.
Using 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

Playing certain video formats may require Video Station or CAYIN Media Player to be installed from App Center.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Play**. **d.** Select a resolution.
Using the context menu	**a.** Right-click the file. **b.** Select **Play**. **c.** Select a resolution.

File Station plays the selected file using Media Viewer.

Playing a video file using CAYIN MediaSign Player

CAYIN MediaSign Player is a third-party web media player. You must install CAYIN MediaSign Player from App Center and have an activated license to play video files.

> **Note**
> CAYIN MediaSign Player can be enabled and disabled using Multimedia Services.

1. Open File Station.
2. Locate the file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Click **Play with CAYIN MediaSign Player**.

Method	Steps
Using the context menu	**a.** Right-click the file. **b.** Click **Play with CAYIN MediaSign Player**

File Station plays the selected file using CAYIN MediaSign Player.

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
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Play**.
Using 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 a Network Media Player

This task requires that you install Media Streaming Add-on from App Center.

1. Open File Station.
2. Locate the file.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click on the toolbar. **c.** Select a 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.** Hover the mouse pointer over **Streaming to**. **d.** Under **Network Media Player**, select a media player.
Using the context menu	**a.** Right-click the file. **b.** Hover the mouse pointer over **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 or folder to the transcoding folder

The transcoding folder is a system folder that stores transcoded files. . Transcoded files can be added to the transcoding folder manually or automatically via Background Transcoding. For more details, see Transcoding.

Important

- File Station cannot convert video files to a higher resolution than the original. If a higher resolution is selected, File Station automatically transcodes the file at the original resolution.
- You must enable transcoding in the Multimedia Console to complete this task.
- Transcoding certain file formats may require you to install and enable CAYIN MediaSign Player from App Center and activate a CAYIN MediaSign Player license.

1. Open File Station.
2. Locate the file.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Add to Transcode**.
Using 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
   - 1080p FULL HD
   - Original resolution
   - Only audio
5. Optional: Rotate the video.
   - Click  to rotate the video clockwise.
   - Click  to rotate the video counterclockwise.
6. Click **OK**.

File Station adds the transcoded 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
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Cancel/Delete Transcoding**.
Using 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
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Transcode Information**.
Using the context menu	**a.** Right-click the file. **b.** Select **Transcode Information**.

Multimedia Console opens. You can view transcoding tasks and configure related settings.

Keeping a folder or a file in reserved cache

You can keep the most important or the most frequently used data in the reserved cache to enhance access performance. HybridMount is required for this task.

Important
You can only perform this operation for folders in the shared folders mounted via HybridMount. For details on how to use HybridMount and how to mount cloud services, see HybridMount Help.

1. Open File Station.
2. Select a mounted shared folder.
3. Select a folder or file.
4. Choose one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Always Keep in Reserved Cache**. A confirmation message appears. **c.** Click **OK**.
Using the context menu	**a.** Right-click the selected item. **b.** Select **Always Keep in Reserved Cache**. A confirmation message appears. **c.** Click **OK**.

File Station keeps the selected folder or file in the reserved cache.

Folders or files in the reserved cache can have one of the following statuses.

Status Icon	Description
	This file or folder is only stored in the cloud
	File Station is downloading this file or folder.
	File Station has encountered an error when downloading this file or folder.
	File Station has cached and is uploading this file or folder.
	File Station has cached and placed this file or folder in the upload queue.
	File Station has encountered an error when uploading this file or folder.

Status Icon	Description
	This file or folder has been cached and synced and will always be kept in the reserved cache.
	This file or folder has been cached and synced.
	This file or folder has been cached and synced but marked as low priority. When the cache space is insufficient, File Station will remove files or folders that are the least recently accessed.
	This file or folder is ignored and not uploaded to the cloud. File Station ignores and skips temporary system files during the sync process.

Converting Apple iWork files to Microsoft Office files

To use this feature, you need to enable a valid CloudConvert API key in **File Station** >  > **Settings** > **Third-party Service**.

For more information, see https://www.qnap.com/en/how-to/faq/article/how-to-get-an-api-key-from-cloudconvert.

1. Open File Station.
2. Locate the iWork file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click  . **c.** Select **Convert with CloudConvert**.
Using the context menu	**a.** Right-click the file. **b.** Select **Convert with CloudConvert**.

   The **CloudConvert Authentication** window appears.

4. Specify your CloudConvert API key.
5. Click **OK**.
   File Station converts the Apple iWork file to Microsoft Office file folder.

Removing a folder from reserved cache

You can remove folders from the reserved cache.

Important
You can only perform this operation for folders in the shared folders mounted via HybridMount. For details on how to use HybridMount and how to mount cloud services, see HybridMount Help.

1. Open File Station.
2. Select a mounted shared folder.
3. Locate one or more folders.
4. Choose one of the following methods.

Method	Steps
Using the toolbar	a. Select one or more folders. b. Click  . c. Select **Do Not Keep in Reserved Cache**. A confirmation message appears. d. Click **OK**.
Using the context menu	a. Select one or more folders. b. Right-click the folder. c. Select **Do Not Keep in Reserved Cache**. A confirmation message appears. d. Click **OK**.

File Station searches

This section describes tasks related to finding your files and folders on File Station.

Searching for files and folders

You can search for files and folders anywhere on the NAS. To search the contents of files, see Using content search to search for file content.

1. Open File Station.
2. On the right side of the search bar, click ▾.
A drop-down search box appears.

3. Specify at least one of the following fields.

Field	Description
Name	Searches by file or folder name.
Type	Searches a file or folder of a specific type.
Location	Searches for files and folders in a specific mount.
Modified Date	Searches before, on, or after a specific date or a date within a range.
Size	Searches for files and folders greater than or less than a specified size.
Owner/Group	Searches for files and folders in the specified category.

4. Click **Search**.

Using content search to search for file content

File content search allows you to search for specific content inside files.

> **Note**
> You need to install and enable Qsirch from App Center to enable this feature.

1. Open File Station.
2. On the right side of the search bar, click ▾.
   A drop-down search box appears.
3. Click the toggle button.
4. Specify at least one of the following fields.

Field	Description
Keyword	Searches for content using a keyword.
Type	Searches a file or folder of a specific type.
Location	Searches for files and folders in a specific mount.
Modified Date	Searches before, on, or after a specific date or a date within a range.
Size	Searches for files and folders greater than or less than a specified size.

5. Click **Search**.

Using the Smart File Filter to search for files and folders

The **Smart File Filter** allows you to apply a set of search criteria to all your data within the current folder. When you open a folder, this feature automatically filters your files and any subfolders by the search criteria.

> **Note**
> Smart File Filter will search file or subfolder within the current parent folder. Use basic or advanced search to search for data in a specific folder.

1. Open File Station.
2. Near the top-right corner, click .
   The **Smart File Filter** screen appears.
3. Specify at least one of the following fields.

Field	Description
Name	Searches by file or folder name.
Size	Searches for files and folders greater than or less than a specified size.
Modified Date	Searches before, on, or after a specific date or a date within a range.
Owner/Group	Searches for files and folders in the specified category.

4. Click **Search**.
   File Station turns on the **Smart File Filter** and filters by the specified criteria.

Other tasks

This section describes miscellaneous tasks that you can perform on File Station.

Removing background tasks

You can remove or stop unnecessary background tasks.

1. Open File Station.
2. Click .

   > **Tip**
   > The **Task** tab displays every task. The **Upload** tab only displays upload tasks.

3. Locate a task to remove.

4. Click ⊠.
   File Station removes the task.

> **Tip**
> To remove all tasks, click **Delete All**. To remove all completed tasks from the **Upload** tab, click **Remove All Complete Tasks**.

Modifying general settings

1. Open File Station.
2. Click ⋮ on the top-right corner.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **General** tab.
5. Modify the following settings.

Option	Description
Show hidden files on NAS	File Station displays files and folders.
Allow all users to create shared links	All users can share data from the NAS using shared links.
Show 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 transcode	File Station prevents non-administrators from using on-the-fly transcoding.
Track file and folder access	File Station allows users to track file or folder access and view information in Access Logs.

6. Click **Close**.

Modifying file transfer settings

1. Open File Station.
2. Click ⋮ on the top-right corner.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **File Transfer** tab.
5. Under **Duplicate File Name Policy**, specify policies for handling duplicate files.

Scenario	Policy
When uploading files	• **Always ask me** • **Rename duplicate files** • **Skip duplicate files** • **Overwrite duplicate files**
When copying or moving files	• **Always ask me** • **Rename duplicate files** • **Skip duplicate files** • **Overwrite duplicate files**

6. Optional: Select **Always merge all file transfer processes into one task**.
7. Under **Google Drive File Transfer Policy**, specify policies for handling Google Drive files.

Scenario	Policy
When downloading or moving Google Drive files	• Always ask me • Download as Microsoft Office file formats (.docx, .pptx, .xlsx) • Keep Google Drive file formats
When downloading a single Google Drive file to my PC	• Always ask me • Download as Microsoft Office file formats (.docx, .pptx, .xlsx) • Keep Google Drive file formats

8. Click **Apply**.
9. Click **Close**.

Modifying multimedia settings

1. Open File Station.
2. Click ⋮ on the toolbar.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **Multimedia** tab.
5. Modify the following settings.

Option	Description
Support multimedia playback and thumbnail display	File Station allows multimedia playback and displays thumbnails for media files. **Note** To enable this feature, you must install and start Multimedia Console from the App Center, and make sure thumbnail generation services work normally in Multimedia Console.
Always display the 360° panoramic view button on the viewer	File Station permanently displays the 360° panoramic view button without checking the file metadata.

6. Click **Close**.

Modifying document settings

1. Open File Station.
2. Click ⋮ on the top-right corner.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **Documents** tab.
5. Optional: Under **Support Document Thumbnail Display**, select one of the following options:

Important
This feature requires Qsirch. You can install it from the App Center.

Option	Description
Do not display	File Station doesn't display or generate thumbnails for documents.
Manually select a document to generate	Users must manually generate thumbnails for documents. To do so, right-click a file in File Station and select **Thumbnail** > **Display Document Thumbnail**. After generating a document thumbnail, you can also manually regenerate or delete the thumbnail.
Automatically generate	File station automatically generates thumbnails for the specified file formats. • PDF (pdf) • Word (docx, doc, dotx, dot, rtf, docm, dotm) • Excel (xlsx, xls, xltx, xlt) • PowerPoint (pptx, ppt, potx, pot, ppsx, pps, pptm, potm, ppsm) • EML (eml)

6. Under **Microsoft Office File Policy**, specify policies for handling Microsoft Office files.

File Format	Policy
For .doc, .ppt, .xls files	• Always ask me • View in Google Docs • Open with Chrome Extension • Open with web browser
For .docx, .pptx, .xlsx files	• Always ask me • Edit with Office Online • View in Google Docs • Open with Chrome Extension • Open with web browser

7. Specify commercial or individual use for Office Online.

Note

For commercial use, you need to sign up for Office 365. You will be redirected to the Office 365 interface when opening a file with Office Online.

8. Click **Apply**.
9. Click **Close**.

Modifying file operations settings

1. Open File Station.
2. Click ⋮ on the top-right corner.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **File Operations** tab.
5. Optional: Select **Always keep SMB file attributes**.

   Note
   Enabling this feature may affect file access speed.

6. Click **Apply**.
7. Click **Close**.

Modifying third-party service settings

You can convert Apple iWork file formats to Microsoft Office file formats using CloudConvert. The converted files will be stored in the same folder with source files.

You can also see the linked account and its remaining credits.

1. Open File Station.
2. Click ⋮ on the top-right corner.
3. Select **Settings**.
   The **Options** window appears.
4. Go to the **Third-party Service** tab.
5. Acquire your CloudConvert API key.

   Tip
   For details, see the tutorial: https://www.qnap.com/go/how-to/faq/article/how-to-get-an-api-key-from-cloudconvert.

6. Paste your CloudConvert API key.
7. Click **Apply**.

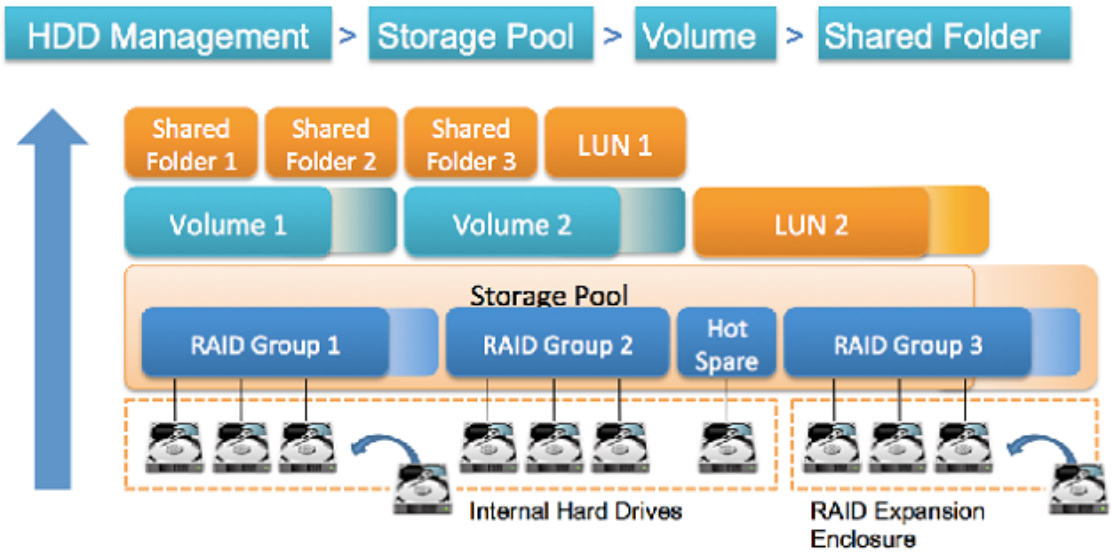
7. Storage & Snapshots

> **Note**
> This utility is only accessible to administrators and users with the System Management role.

Storage & Snapshots is a QTS utility that helps you create, manage, and monitor storage on your NAS. With Storage & Snapshots you can perform the following tasks:

- Create RAID groups, storage pools, and shared folders.
- Monitor storage usage and access speeds.
- Back up data using snapshots.
- Accelerate the performance of your NAS by creating an SSD cache.
- Specify which hosts (computers, servers, other NAS devices) can access the NAS.

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.

Object	Description	Details
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.
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 speed of RAID operations (rebuild, migration, scrubbing, and sync) for each RAID group. 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.
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. SSD trim is only performed on SSDs that belong to a RAID 0, RAID 1, or RAID 10 group. By default, the operations are scheduled to run daily at 2:00 AM. **Tip** We recommend enabling this feature if you have thin volumes or SSD RAID groups of type RAID 0, RAID 1, or RAID 10. **Note** To reclaim space on a thin LUN, the reclaim must be run on the iSCSI client.

Setting	Description
Scheduled File System Check	Enable this feature to scan and automatically fix all volumes that have file system errors at a later date.

Disk and device global settings

Setting	Description
Predictive Migration	Enable this feature to regularly monitor disk health and allow QTS to automatically replace a disk before it fails. If any of the specified events occur, 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.
Use SSD estimated remaining life with S.M.A.R.T. disk migration	Enable this feature to migrate data from an SSD to a spare disk and rebuild the RAID group when the SSD's estimated remaining life falls below 5%.
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.
Check for expansion unit firmware updates at login	Enable this feature to automatically check online for newer firmware for each expansion unit connected to the NAS. If QTS detects newer firmware, it will ask whether you want to install it.
Share my disk analysis data with QNAP	Enable this feature to send de-identified disk analysis data and NAS system information to QNAP to improve future products. QNAP does not collect any user data. You can opt out of this program at any time. If the app DA Drive Analyzer is installed, enabling this setting sends disk analysis data that is linked to your QID to QNAP. **Note** Disabling this setting causes the app DA Drive Analyzer to stop working.
SSD Estimated Life Warning	Enable this feature to change the disk status of an SSD to "Warning" when its estimated life is lower than the specified threshold.

Snapshot global settings

Setting	Description
Smart Snapshot Space Management	Enable this feature to automatically delete snapshots in a storage pool when free space (guaranteed snapshot space plus free storage pool space) is less than 32 GB. This feature deletes the oldest snapshots first until there is at least 40 GB of free space. Enabling this feature reduces the chance of service interruption due to insufficient storage space. You can choose one of the following policies to apply to each volume/LUN in a storage pool when free space in the pool is insufficient: • **Delete all snapshots (release maximum space for service continuity)** • **Delete all except the newest snapshot (maintain data protection)** • When this policy is selected and the snapshot retention policy for a volume/LUN is set to **Smart Versioning**, the system retains the newest snapshot of each time interval when deleting snapshots. For details, see Configuring a snapshot retention policy. **Note** This feature does not delete permanent snapshots. **Important** If QTS is unable to free at least 32 GB of snapshot space, the system stops creating new snapshots.
Snapshot Access in File Station	You can enable the following settings for viewing and accessing snapshots in dedicated folders in File Station: • **Root snapshot folder (for authorized users)**: Makes the `Snapshot` root folder visible to administrators and users with the System Management role. This folder allows authorized users to view and manage all snapshots on the NAS. • **Snapshot folder in each shared folder**: Makes the `@Recently-Snapshot` folder visible in each shared folder. This folder allows users to view all snapshots in the shared folder when connecting via SMB, CIFS, or AFP.

Setting	Description
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** **Note** This setting does not apply to Snapshot Vault. For Snapshot Vault, you can set the maximum number of snapshots when configuring a Snapshot Replica job. For details, see Creating a Snapshot Replica job.
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.
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 storage 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

- For compatibility reasons, PCIe form-factor SSDs and PCIe M.2 SSDs installed in third-party adapter cards cannot be used to create storage pools and static volumes.
- If you are already using NVMe PCIe SSDs for data storage, then your existing storage configuration will not be affected after upgrading to the latest version of QTS.

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	Third-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

Note

QTS supports Seagate dual-actuator HDDs. In Storage & Snapshots, these disks are labeled with the tag `Seagate DA`.

Disk management

You can manage disks at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**. Select a disk to view its status and hardware details.

Disk statuses

You can view various disk statuses by going to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.

Status Name	Description
Health Status	The health status of the disk • `Good`: The disk is normal. • `Warning`: The system has detected S.M.A.R.T. errors. Run a full S.M.A.R.T. test and a disk scan. • `Error`: The system has detected I/O errors. You must replace the disk immediately. • `None`: There is no disk in the drive bay or slot.
Status	The behavioral status of the disk • `Ready`: The disk is ready. • `Migrating`: The disk is replacing another disk in a RAID group. • `Rebuilding`: The disk's RAID group is rebuilding. • `Removing`: The system is removing the disk from its RAID group. • `Bad blocks scanning`: The system is scanning the disk for bad blocks. • `Secure erase`: The system is permanently erasing all data on the disk. • `Inactive`: The disk is not connected.
Used Type	How the disk is used by the system • `Data`: The disk is being used for data storage. • `Spare`: The disk is configured as a spare disk. • `Free`: The disk has not been assigned any purpose. • `Cache`: The disk is being used in the SSD cache. • `None`: There is no disk in the drive bay or slot

Disk information

To view information on a disk, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select the disk, and then click **Information**.

Information	Description
Disk Health Status	The general health status of the disk For details, see Disk statuses.
Manufacturer	The manufacturer of the disk
Model	The disk model
Disk Capacity	The capacity of the disk, in both binary and decimal formats • Binary format assumes that 1 GB = 1,073,741,824 bytes. This is the true capacity of the disk and is used by computers and operating systems such as QTS. • Decimal format assumes that 1 GB = 1,000,000,000 bytes. This format is used by disk manufacturers and appears in advertising, on the disk's box, and in the disk's hardware specifications. • Due to differences in the number of bytes per gigabyte, a disk's binary capacity will be slightly lower than its decimal capacity. For example, a disk advertised as 500 GB (decimal) has a true capacity of 456 GB (binary).
Bus Type	The interface that the disk uses
Supported Bus Types	The disk types the drive bay supports For example, an internal M.2 SSD slot might support SATA and NVMe SSDs.
Status	The behavioral status of the disk For details, see Disk statuses.
SED Status	The encryption status of the self-encrypting drive (SED) For details, see SED status.
Mode	The power mode (spinning state) of the disk The disk can be active (spinning) or in standby (spindown).
Current Speed	The speed at which the disk is connected to the enclosure
Maximum Speed	The maximum transfer speed supported by the drive bay or slot that the disk is installed in
Temperature	The current temperature of the disk Disk temperature is retrieved from the disk's firmware using S.M.A.R.T.
Disk Access History (I/O)	• Good: QTS has not detected any I/O errors on the disk. • Error: QTS has detected one or more I/O errors on the disk.

Information	Description
Estimated Life Remaining	The remaining life of the disk, as calculated by the disk's firmware. When the value reaches 0, you should replace the disk. This information is only available for solid-state drives.
SSD Features	Features pertaining to solid-state drives

Disk health

To view health information on a disk, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select the disk, and then click **Health**. Click **View Details** to view all health information.

Tab	Description
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.
IronWolf Health Management	IronWolf Health Management (IHM) monitors environment and usage conditions, such as temperature, shock, and vibration, and suggests preventative actions to ensure optimal performance for Seagate IronWolf disks. Run an IHM test to view the disk's IHM status. **Note** This feature is unavailable when there is no system volume. The IHM test is only available for HDDs. • **Test**: Run an IHM test now. • **Set Schedule**: Run the IHM test periodically on a schedule. • **Statistics**: View IHM data read/write statistics.
WDDA	Western Digital Device Analytics (WDDA) is a feature available to certain Western Digital drives. This feature monitors drive health and provides recommended actions when drive issues are detected.
SMART Information	Displays S.M.A.R.T. disk information and supported attributes. **Important** If the value of a S.M.A.R.T. attribute reaches the threshold set by the disk manufacturer or a predefined threshold determined by QTS, the SMART attribute's status changes to `Warning`.

Tab	Description
Test	Run a S.M.A.R.T. disk self-test. • **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.
Settings	Disk settings can be applied individually, or to multiple disks at once. • **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. • **IronWolf Health Management**: Schedule a daily IHM test for the disk. The results are saved in the selected shared folder, and are displayed on the **IronWolf Health Management** 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).
Advanced	Displays advanced settings. • **Native Command Queuing (NCQ)**: Enhances the read and write performance of the disk. **Note** • This setting is only available for SATA disks. • To disable this setting, contact QNAP support. • To prevent the disk from becoming undetectable, this setting is automatically disabled and cannot be enabled if the system detects NCQ timeout errors.

Disk actions

Action	User Action
Detach	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Detach**. Removes the disk from its RAID group. The group must be of type: RAID 1, RAID 5, RAID 6, RAID 10.
Disable spare	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Disable Spare**. Unassigns the disk as a global hot spare.
Locate	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Locate**. Prompts the drive LEDs to blink so that you can locate the drive in a NAS or expansion unit.
Manage free disks	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks** > ⋮ > **Manage Free Disks**. Opens a window that helps you decide what to do with existing free disks and provides links to further actions.
Replace	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Replace**. Replaces the disk with a spare disk. After all data on the selected disk is copied to the spare disk, the selected disk is safely detached from the RAID group and the system.
Scan for bad blocks	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Scan for Bad Blocks**. Scans 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**.
Set as enclosure spare	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Set as Enclosure Spare**. Assigns the disk as a global hot spare for all RAID groups within the same enclosure (NAS or expansion unit). For details, see Configuring an enclosure spare disk.

Action	User Action
Securely erase	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Action** > **Secure Erase**. Permanently erases all data on a disk. For details, see Securely erasing a disk.
View disk health information	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Health**. Displays disk S.M.A.R.T. information. For details, see Disk health.
View disk information	Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a disk, and click **Information**. Displays disk details, including the disk manufacturer, model, serial number, disk capacity, bus type, firmware version, ATA version, and ATA standard.

Securely erasing a disk

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. Only administrators can perform this task.

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

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.
2. Select a free disk.
3. Click **Action**, and then select **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 your password.

   Note
   You must be logged in as an administrator.

9. Click **Apply**.

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

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 manually

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
2. Click ⋮ and select **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**.

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**.

Testing disk performance on a schedule

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
2. Click ⋮ and select **Performance Test**.
   The **Performance Test** screen appears.
3. Set **Weekly Test** to **On**.
   A confirmation message appears.
4. Click **OK**.

QTS runs a sequential read test for all disks every Monday at 6.30am, and then displays the results on the **Performance Test** screen.

Disk failure prediction

QTS provides failure prediction for your disks so you can replace them in time to prevent sudden data loss. The prediction service is powered by ULINK Technology, Inc.'s DA Drive Analyzer, a third-party application and cloud AI engine that tracks disk analysis data to monitor disk health.

For more information on DA Drive Analyzer, visit the following links:

- QNAP DA Drive Analyzer
- ULINK DA Drive Analyzer

Activating disk failure prediction

To activate disk failure protection on a device, you must install DA Drive Analyzer on the device and enable sharing disk analysis data.

QNAP provides a free perpetual license seat for a single disk on each device. To use predictions on more disks, you must purchase additional licenses.

1. Install DA Drive Analyzer.
   a. Go to App Center, and then click  .
   A search box appears.
   b. Enter `DA Drive Analyzer`.
   The DA Drive Analyzer application appears in the search results.
   c. Click **Install**.
   A confirmation message appears.
   d. Click **Yes, I agree**.
   The system installs DA Drive Analyzer.
2. Log in to DA Drive Analyzer.
   a. Open DA Drive Analyzer.
   The **Policy Agreement** window opens.
   b. Click **Accept**.
   The **Log In** window appears.
   c. Click **Log in**.
   The **QNAP Account** page appears.
   d. Enter a QNAP ID and password, and then click **Sign in**.

   Tip
   This QNAP ID will be the Main Registered User (MRU) in DA Drive Analyzer. You can use the same MRU on multiple QNAP devices. In the application, the MRU can designate other QNAP IDs as viewers.
   The MRU and designated viewers can also log in to the ULINK DA Portal (accessible through DA Drive Analyzer). The DA Portal contains more advanced information and functions, such as the ability to set up email alerts and monitor disks on multiple devices.

   The page closes and the **Overview** page appears in DA Drive Analyzer.

3. Optional: Purchase and activate licenses.

   Note
   QNAP provides a free perpetual license seat for a single disk on each device. You can skip this step if you want to try out the service first. To use predictions on more disks, you must purchase additional licenses.

   a. In DA Drive Analyzer, click **Buy License**.
   The **Purchase License for Selected Slots** window opens.

   b. Select **Add to cart** for one or more disks.

   c. Click **Purchase**.
   The DA Drive Analyzer license page opens in a new browser window.

   d. Select a license, and then review the price.

   e. Click **Checkout Now**.
   The purchase summary page appears in your web browser.

   f. Follow the on-screen instructions to complete the purchase.
   Once the purchase is complete, the system proceeds to activate the purchased license in the same browser window.

   g. Wait for the system to complete the activation process.

      Important
      Do not close this window until the **Close** button appears.

   h. Click **Close** after activation is complete.
   The browser returns to the DA Drive Analyzer window.
   DA Drive Analyzer automatically assigns the new license seats to the selected disks.

4. Optional: Modify license seat assignments.

   a. In DA Drive Analyzer, click **License Seat Assignment**.
   The **License Seat Assignment** window opens.

   b. Remove or assign license seats.

Action	User Action
Remove a license seat from a disk	Under **License Seat**, click the drop-down menu and select **--**.
Assign an available license seat to an unlicensed disk	Under **License Seat**, click the drop-down menu and select an available seat.

Action	User Action
Automatically assign all available license seats sequentially to unlicensed disks	Click **Auto-assign**.

5. Share your disk analysis data with QNAP.
   a. Go to **Storage & Snapshots** >  > **Disk / Device**.
   b. Enable **Share my disk analysis data with QNAP**.
   c. Click **Apply**.

QNAP starts uploading disk analysis data once per day to ULINK's cloud AI engine.

Note
Predictions are available after analyzing one day of uploaded data and one extra day of synchronization.

Tip
To view disk failure prediction statuses, see Disk failure prediction status.

Disk failure prediction status

To view the disk failure prediction status of a disk, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks** and check the `ULINK DA` column. To view further information, click the disk and then click **Prediction** in the bottom pane.

You can also view disk failure prediction statuses in DA Drive Analyzer.

Status	Description
Normal	The disk is functioning normally.
Warning	The disk has a 70% risk of failure.
Critical	The disk has a 90% risk of failure.
Faulty	The disk is defective.
Data Analysis in Progress	The disk data is being analyzed. To provide failure prediction, the cloud AI requires 14 days of data within the last 20 days. An additional day is required to synchronize the disk health status with ULINK DA Drive Analyzer.

Status	Description
Unlicensed	The disk is unlicensed. To obtain failure prediction for the disk, you must assign a license seat to the disk.
Unsupported	The disk is not supported for failure prediction.

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.

	Volume Type		
	Static	**Thick**	**Thin**
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.
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

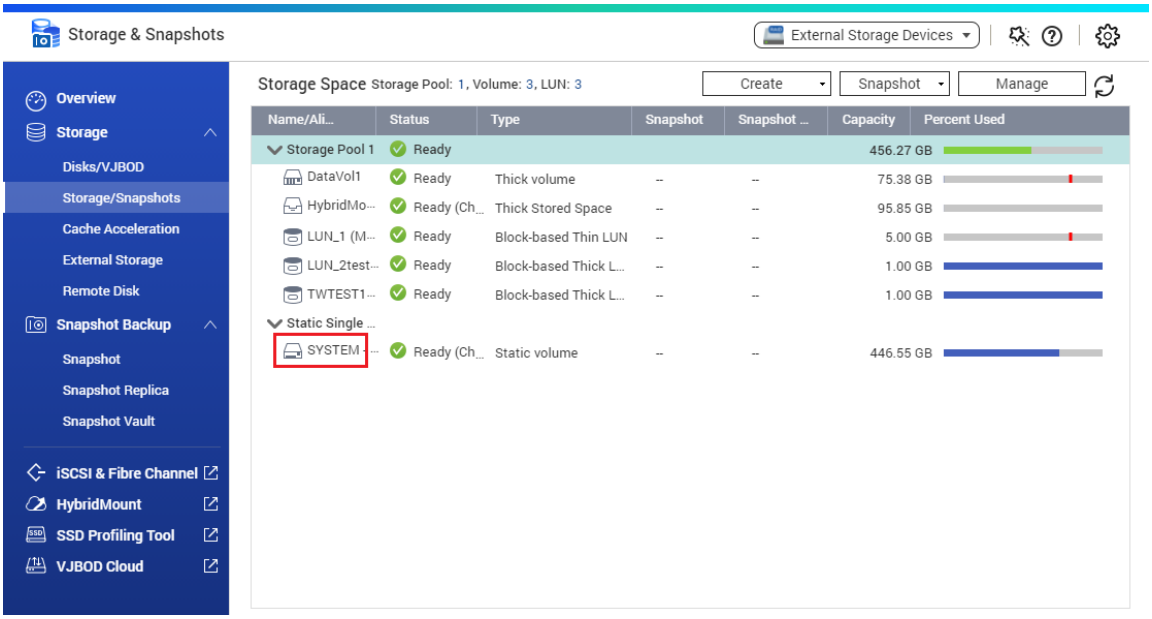
QNAP recommends replacing legacy volumes with newer volumes. To replace a legacy volume, back up all data, create a new thick, thin, or static volume, and then restore the data to the new volume.

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 10 GB. 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.

Volume configuration examples

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.

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 encounter 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 scenarios

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 movie files. Random-write performance is slightly lower than a single static volume.
Contain-erizing 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 how 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.
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

You can create a maximum of 128 volumes. QNAP recommends keeping the total number of volumes low for optimal performance.

Creating a static volume

To create a SED secure static volume, see Creating a SED secure static volume.

1. Go to **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**.

   Tip

   - Click **Detailed Comparison** to view feature differences between the volume types in a new window. You can select a different volume type to see the corresponding description and graph, and also apply a new selection.
   - To create a thick or thin volume, see Creating a thick or thin 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 becomes inaccessible until the expansion unit is reconnected.

6. Select one or more disks.

Important

- For data safety, you cannot select disks that have the status `Warning`.
- The status `In Use` means that a disk is currently formatted as an external disk, and may contain current user data.
- If you select a disk with the status `In Use`, QTS will temporarily stop all disk storage services on the NAS in order to unmount the disk, and then delete all data and partitions on the disk.

Warning
All data on the selected disks will be deleted.

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
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 unsure of which option to choose.
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 disk failure protection.

9. Optional: Select the number of RAID 50 or RAID 60 subgroups.
   The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.

   - A higher number of subgroups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
   - A lower number of subgroups 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 subgroups 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 (-), underscore (_)

12. Optional: Encrypt the volume.
    QTS encrypts all data on the volume with 256-bit AES encryption.

    a. Specify an encryption password.
       The password must contain 8 to 32 characters, with any combination of letters, numbers, and special characters. Spaces are not allowed.

       Warning
       If you forget the encryption password, all data will become inaccessible.

    b. Verify the encryption password.
    c. Optional: Select **Auto unlock on startup**.
       This setting enables the system to automatically unlock and mount the encrypted volume whenever the NAS starts, without requiring the user to enter the encryption password or encryption key file.

       Warning
       Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

13. 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 SSD Profiling Tool from App Center.

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.
Accelerate performance with SSD cache	QTS adds data from this volume to the SSD cache to improve read or write performance.	-
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the user account that creates the shared folder has read/write access to the folder. **Note** This setting is only available when logged in as "admin".	• Specify a folder name. • Select **Create this folder as a snapshot shared folder**. A snapshot shared folder enables faster snapshot creation and restoration.
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.	Select a value.

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 volume

1. Go to **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 a storage pool.
   You can select an existing storage pool or create a new storage pool immediately.
4. Optional: Create a new storage pool.
   a. Click **Create**, and then select **New Storage Pool**.
      The **Create Storage Pool Wizard** window opens.
   b. Complete the instructions in Creating a storage pool, starting from step 3.

   QTS creates the storage pool. The **Create Storage Pool Wizard** window closes.
5. Select a volume type.
   - Thick Volume
   - Thin Volume

   Tip
   - Click **Detailed Comparison** to view feature differences between the volume types in a new window. You can select a different volume type to see the corresponding description and graph, and also apply a new selection.
   - To create a static volume, see Creating a static volume.
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 (-), 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. Optional: Encrypt the volume.
   QTS encrypts all data on the volume with 256-bit AES encryption.

   a. Specify an encryption password.
      The password must contain 8 to 32 characters, with any combination of letters, numbers, and special characters. Spaces are not allowed.

      Warning
      If you forget the encryption password, all data will become inaccessible.

   b. Verify the encryption password.

   c. Optional: Select **Auto unlock on startup**.
      This setting enables the system to automatically unlock and mount the encrypted volume whenever the NAS starts, without requiring the user to enter the encryption password or encryption key file.

      Warning
      Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

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.
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 user account that creates the shared folder has read/write access to the folder. **Note** This setting is only available when logged in as "admin".	• Specify a folder name. • Select **Create this folder as a snapshot shared folder**. A snapshot shared folder enables faster snapshot creation and restoration.
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.	Select a value.

11. Click **Next**.
12. Optional: Select **Enable snapshot schedule and snapshot retention**.
    This step is only available when you are creating a thin volume.

    Note
    If this setting is selected, QTS creates a default snapshot schedule and snapshot retention policy. You can configure or change these settings at any time.
    For details, see the following:

    - Configuring a snapshot schedule
    - Configuring a snapshot retention policy
13. Click **Next**.
14. Click **Finish**.

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

Volume management

Deleting a volume

Note

- To delete a VJBOD Cloud volume, use the VJBOD Cloud app.
- To delete a HybridMount volume, use the HybridMount app.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a volume.

   Warning
   All data on the selected volume will be deleted.

3. Click **Manage**.
   The **Volume Management** window opens.
4. Select **Action** > **Remove**.
   The **Volume Removal Wizard** window opens.
5. Click **Apply**.

Configuring a volume space alert

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a volume.
3. Click **Manage**.
   The **Volume Management** window opens.
4. Click **Actions**, and then select **Set Threshold**.
   The **Alert Threshold** window opens.
5. Enable space alerts.
6. Specify an alert threshold.
   QTS issues a warning notification when the percentage of used space is greater than or equal to the specified threshold.
7. Click **Apply**.

Volume file system check

A file system check scans for and automatically repairs errors in the file system of a thick, thin, or static volume. QTS will prompt you to start a file system check if it detects file system errors on one or more volumes. You can also run a file system check manually or schedule a one-time check.

Running a file system check manually

Warning

- A volume is unmounted and becomes inaccessible while its file system is being checked.
- This process might take a long time, depending on the size of the volume.

Important

QTS will scan the specified volume, even if QTS has not detected any errors on the volume's file system.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a volume.
3. Click **Manage**.
   The **Volume Management** window opens.
4. Click **Actions**, and then select **Check File System**.
   The **Check File System** window opens.
5. Click **OK**.

QTS creates a background task for the file system check. The status of the volume changes to `Checking...`.

Running a one-time file system check on a schedule

Warning

- A volume is unmounted and becomes inaccessible while its file system is being checked.
- This process might take a long time, depending on the size of the volume.

Important

QTS will only scan the specified volume if it has detected errors on the volume's file system.

1. Open **Storage & Snapshots**.
2. Click  .
   The **Global Settings** window appears.
3. Click **Storage**.
4. Enable **Scheduled File System Check**.

5. Specify a date and time.
6. 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.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.
3. Click **Manage**.
   The **Volume Management** window opens.
4. Select **Action** > **Resize Volume**.
   The **Volume Resizing Wizard** opens.
5. Specify a new capacity for the volume.
   Capacity can be specified in megabytes (MB), gigabytes (GB) or terabytes (TB).

6. Optional: Click **Set to Max**.
   Sets the new volume capacity to the maximum available size. This option is only available for thick volumes.
7. Click **Apply**.
   If you are shrinking the volume, a confirmation message appears.
8. 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 greater than or equal to the smallest disk in the group.
   - The status of the RAID group that you want to expand is `Ready`.
2. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
3. Select a static volume.
4. Click **Manage**.
   The **Volume Management** window opens.
5. Select **Action** > **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, or 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 SSD Profiling Tool 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 QTS writes data to a RAID group until the group 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a static volume.
3. Click **Manage**.
   The **Volume Management** window opens.

4. Select **Action** > **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 becomes inaccessible until the expansion unit 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. 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 SSD Profiling Tool 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 combines many physical disks into one large pool of storage space. Disks in the storage pool are joined together using RAID technology to form RAID groups. Storage pools may contain more than one RAID group.

Using storage pools provides the following benefits:

- Multiple volumes can be created in 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 installed 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 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 groups can be striped together using RAID 0 to form a RAID 50 or RAID 60 storage pool.

Creating a storage pool

1. Go to **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**, and then select **New Storage Pool**.

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

3. Optional: Enable Qtier.
   Qtier is an automated-tiering storage solution that automatically moves frequently accessed data to high-performance drives for greater read and write performance, and infrequently accessed data to higher-capacity drives for more cost-effective storage. Once Qtier is enabled, it cannot be disabled. You can choose to enable Qtier later.
   For details, see Qtier.
4. Optional: Enable SED encryption and create a SED secure storage pool.
   You must have free SEDs on the NAS.
   For details, see the following topics:
   - Self-encrypting drives (SEDs)
   - Creating a SED secure storage pool
5. Click **Next**.
6. 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 becomes inaccessible until the expansion unit is reconnected.
7. Select one or more disks.

   Important

   - For data safety, you cannot select disks that have the status `Warning`.
   - The status `In Use` means that a disk is currently formatted as an external disk, and may contain current user data.
   - If you select a disk with the status `In Use`, QTS will temporarily stop all disk storage services on the NAS in order to unmount the disk, and then delete all data and partitions on the disk.
   - The number of disks you can select depends on the RAID type you want to select. For details, see the following:
     - RAID types
     - QNAP RAID Calculator
   - If you select multiples of three disks and select Triple Mirror for the RAID type, every three disks will form an individual RAID group in the storage pool. You can select a maximum of 15 disks with Triple Mirror.

   Warning
   All data on the selected disks will be deleted.

8. If you enabled Qtier, click **OK**.
9. Select a RAID type.
   QTS displays all available RAID types and automatically selects the most optimized RAID type.

   Tip
   Use the default RAID type if you are unsure of which option to choose.
   For details, see RAID types.

10. 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 subgroups share the same spare disk.
    a. Identify the disk to use as a hot spare.
    b. Under **Mode**, click **Data**.
    c. Select **Spare**.
11. Optional: Select the number of RAID 50 or RAID 60 subgroups.
    The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.
    - A higher number of subgroups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
    - A lower number of subgroups 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 subgroups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

12. If you enabled Qtier, select disks for at least one more tier and configure the RAID type and optionally a spare disk for each tier.
    For details, see Qtier requirements.
13. Click **Next**.
14. 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 SSD Profiling Tool from App Center.

15. Optional: Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
16. Optional: Configure pool guaranteed snapshot space.
    Pool 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.
17. If you enabled SED encryption, configure the SED settings.
    a. Specify the encryption password.
    The encryption password must consist of 8 to 32 characters from any of the following groups:
    - Letters: A to Z, a to z
    - Numbers: 0 to 9
    - Special characters: Any except for space ( )

    Warning
    Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable.

    b. Optional: Select **Auto unlock on startup**.
    This setting enables the system to automatically unlock and mount the SED pool whenever the NAS starts, without requiring the user to enter the encryption password.

    Warning
    Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.
18. Click **Next**.
19. Verify the storage pool information.
20. Click **Create**.
    A confirmation message appears.

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

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

Storage pool management

Storage pool status

Status	Description
Ready	The storage pool is working normally. All RAID groups in the pool have the status `Ready`.
Warning (Degraded)	One or more RAID groups in the storage pool have the status `Degraded`. There are not enough spare disks available to QTS to rebuild all of the RAID groups.
Warning (Rebuilding)	One or more RAID groups in the storage pool have the status `Degraded (Rebuilding)`. QTS is currently rebuilding them due to disk failure.
Warning (Read-Only)	One or more RAID groups in the storage pool have the status `Not Active`. **Note** It might be possible to recover some data from volumes and LUNs.
Warning (Threshold Reached)	Used space in the storage pool is greater than or equal to the alert threshold. **Note** To configure the alert threshold, see Configuring a storage pool space alert.
Warning (Space Low)	The storage pool is running low on space. **Note** Insufficient space might affect data storage, snapshot, and application services. To prevent potential service interruption or issues, free up space or expand the pool capacity. For details, see Increasing free space in a storage pool.

Deleting a storage pool

Only administrators can perform this task.

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

3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Select **Action** > **Remove Pool**.
   A notification window opens.
5. Select **Confirm the removal of every volume/iSCSi LUN/Snapshot Vault on this storage pool**.

   Warning
   All data in the storage pool will be deleted.
6. Click **OK**.
   The **Remove Pool** window opens.
7. Enter your password.

   Note
   You must be logged in as an administrator.
8. Click **OK**.

Configuring a storage pool space alert

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Set Threshold**.
   The **Alert Threshold** window opens.
5. Enable space alerts.
6. Specify an alert threshold.
   QTS issues a warning notification when the percentage of used space is greater than or equal to the specified threshold.
7. Click **Apply**.

Increasing free space in a storage pool

Storage & Snapshots provides a one-stop location where you can perform one or more actions to increase free space in a storage pool.

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

3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Free some space**.
   The **Increase Pool Free Space** window opens.
5. Perform an available action.

> **Note**
> Some options are only available if the storage pool has the corresponding configuration or contains the corresponding storage objects.

Option	User Action
Run a space reclaim to release used space in thin volumes	**Note** The storage pool must have at least one thin volume with reclaimable space. To create reclaimable space in a thin volume, you can delete unwanted files. **a.** Click **Execute**. A dialog box appears. **b.** Click **OK**. The system releases the used space to the storage pool. A dialog box appears. **c.** Click **OK**.
Delete older snapshots	**a.** Select a volume or LUN. **b.** Click **Manage**. The **Snapshot Manager** window opens. **c.** Optional: Click ☰ to change to list view. **d.** Select one or more snapshots to delete. **e.** Click  .

Option	User Action
Release unused pool guaranteed snapshot space	**Note** Pool guaranteed snapshot space is storage pool space that is reserved for storing snapshots. **a.** Click **Manage**. The **Snapshot Settings** window opens. **b.** Select a lower percentage or specify a lower amount of storage pool space to reserve for snapshots. **c.** Click **OK**.
Convert a thick volume to a thin volume	**Important** Converting a thick volume to a thin volume temporarily stops all services on the volume and permanently deletes all snapshots in the volume. **a.** Select a thick volume. **b.** Click **Execute**. The **Convert to Thin Volume** window opens. **c.** Review the information. **d.** Click **Apply**. The system converts the thick volume to a thin volume and releases the freed space to the storage pool.

Option	User Action

Expand the storage pool or release pool over-provisioning space	**a.** Click **Expand**.
	The **Expand Storage Pool Wizard** window opens.
	b. Select one of the following options and complete the wizard:
	• **Create and add a new RAID group**
	For details, see Expanding a storage pool by adding a new RAID group.
	• **Add new disk(s) to an existing RAID group**
	For details, see Expanding a storage pool by adding disks to a RAID group.
	• **Decrease over-provisioning**
	  • Over-provisioning reserves a percentage of SSD storage space on each disk in a RAID group to improve write performance and extend the disk's lifespan.
	  • To determine the optimal amount of over-provisioning for your SSDs, download and run SSD Profiling Tool from App Center.
	  For details, see SSD Profiling Tool.

6. Optional: Perform another available action.
7. Click **Close**.

Storage pool expansion

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 QTS writes data to a RAID group until a group 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a storage pool.

3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Select **Action** > **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

   - You cannot select disks from multiple expansion units.
   - You cannot use the disks from a QNAP JBOD enclosure to expand a storage pool which is located on a different enclosure.
   - If the expansion unit is disconnected from the NAS, the storage pool becomes inaccessible until the expansion unit is reconnected.
8. Select one or more disks.

   Important

   The number of disks you can select depends on the RAID type you want to select. For details, see the following:

   - RAID types
   - QNAP RAID Calculator

   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.
    The designated hot spare automatically replaces any disk in the RAID group that fails.
11. Click **Next**.

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 SSD Profiling Tool 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 storage pool. The capacity of the pool increases after RAID rebuilding is finished.

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 greater than or equal to the smallest disk in the group.
   - The status of the RAID group that you want to expand is `Ready`.
2. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
3. Select a storage pool.
4. Click **Manage**.
   The **Storage Pool Management** window opens.
5. Select **Action** > **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, or RAID 60.
8. Click **Next**.
9. Select one or more disks.

   Important
   The maximum number of disks you can select depends on the RAID type after expansion. Subtract the existing number of disks from the RAID type's maximum total number of disks in order to determine the maximum selectable number of disks. For RAID 50 or 60, further divide this number by the number of sub-groups.

RAID Type	Maximum Total Number of Disks
RAID 5	16
RAID 6	16
RAID 50	30
RAID 60	30

   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 SSD Profiling Tool 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.

Storage pool migration

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

- Files and folders
- Storage configuration
- Snapshots

Storage pool migration requirements

The following requirements apply when migrating a storage pool to a new NAS.

- The two NAS devices must both be running QTS, or both be running QuTS hero. Migration between QTS and QuTS hero is not possible.
- The version of QTS or QuTS hero running on the new NAS must be the same or newer than the version running on the original NAS.

Migrating a storage pool to a new NAS

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Action**, and then select **Safely Detach Pool**.
   A confirmation message appears.
5. Click **Yes**.
   The storage pool status changes to `Safely Detaching...`. After the system finishes detaching the pool, the pool disappears from Storage & Snapshots.
6. Remove the drives containing the storage pool from the NAS.
7. Install the drives in the new NAS.
8. On the new NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
9. Click ⋮ and select **Recover** > **Attach and Recover Storage Pool**.
   A confirmation message appears.
10. Optional: Enter the encryption password.
    You must enter this password if you are using self-encrypted drives (SEDs) with encryption enabled.

11. Click **Attach**.
    The system scans the disks and detects the storage pool.
12. Click **Apply**.

The storage pool appears in Storage & Snapshots on the new 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 performance and redundancy.

Important

- For best performance and space efficiency, you should use disks of the same brand, disk type, and capacity when creating a RAID group.
- If disks with different capacities are combined in one RAID group with disk failure tolerance, 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.
  a. Create a separate RAID group for each capacity.
  b. Combine the RAID groups using storage pools.
- If different types of disk (HDD, SSD, SAS) are combined in one RAID group, the RAID group will function according to the speed of the slowest disk.
- Increasing the number of disks in a RAID group increases the risk of simultaneous disk failure and lengthens rebuild times. For example, a RAID group with 24 drives is 20 times more likely to fail with RAID 6 than with RAID 60. When creating a storage pool with a large number of disks, you should split the disks into sub-groups using RAID 50 or RAID 60.

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)	≥ 2	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, you should use RAID 0 instead.

RAID Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
RAID 0	2 to 16	0	Total combined disk capacity	• Disks are combined together using striping. • RAID 0 offers the fastest read and 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 1	2	1	Half of the total combined disk capacity	• An identical copy of data is stored on each 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 to 16	1	Total combined disk capacity minus 1 disk	• Data and parity information are striped across all disks. • The capacity of one disk is lost to store parity information. • Striping means read speeds are increased with each additional disk in the group. • Recommended for a good balance between data protection, capacity, and speed.

RAID Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
RAID 6	4 to 16	2	Total combined disk capacity minus 2 disks	• Data and parity information are striped across all disks. • The capacity of two disks are lost to store parity information. • Recommended for critical data protection, business and general storage use. It provides high disk failure protection and read performance.
RAID 10	4 to 16 (Must be an even number)	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 and write speeds and high failure protection, but half the total disk capacity is lost. • Recommended for applications that require high random access performance and fault tolerance, such as databases.
RAID 50	6 to 30	1 per disk subgroup	Total combined disk capacity minus 1 disk per subgroup	• 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 Type	Number of Disks	Disk Failure Tolerance	Capacity	Overview
RAID 60	8 to 30	2 per disk subgroup	Total combined disk capacity minus 2 disks per subgroup	• 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 group status

Status	Description
Ready	The RAID group is working normally.
Degraded	One or more disks in the RAID group have failed. The number of disk failures are within the disk failure tolerance of the RAID group. There are not enough spare disks available to QTS to replace all the failed disks.
Degraded (Rebuilding)	One or more disks in the RAID group have failed. The number of disk failures are within the disk failure tolerance of the RAID group. QTS has replaced the failed disks with spare disks, and is now rebuilding the RAID group.
Not active	One or more disks in the RAID group have failed. The number of disk failures exceeds the disk failure tolerance of the RAID group.

RAID disk failure protection

All RAID types except for RAID 0 can tolerate a specific number of disk failures without losing data. When a disk in a RAID group fails, the RAID group status changes to `degraded` and then QTS performs one of the following actions.

Spare Disk Available	Actions
Yes	• QTS automatically replaces the failed disk with a spare disk and then starts rebuilding the RAID group. • The status of the RAID group changes to `rebuilding`, and then changes back to `Ready` after rebuilding has finished.
No	You must replace the failed disk manually. QTS starts rebuilding the RAID group after you have installed a working disk.

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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
3. Select a storage pool or single static volume.
   The storage pool or volume management window opens.
4. Click **Manage**.
5. Select a RAID group.
6. Click **Manage** and select **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, and appear with a `Spare` tag in **Disks/VJBOD** > **Disks**.

Configuring an enclosure spare disk

An enclosure space disk acts as a hot spare for all RAID groups within a single enclosure (NAS or expansion unit). Under normal conditions, the enclosure space 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.

Important

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

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**
2. Select a free disk under an enclosure.
3. Click **Action**, and then select **Set as Enclosure Spare**.
   A confirmation message appears.
4. Click **OK**.

   Warning

   All data on the selected disk will be deleted.

The disk appears as a `Spare`.

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 **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 **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 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 **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 RAID Group**.

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 with an Error status

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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
3. Select a storage pool or single static volume with the status `Inactive`.
4. Click **Manage**.
   The **Storage Pool Management** or **Volume Management** window opens.
5. Select a RAID group with the status `Error`.
6. Click **Manage**, and then select **Recover RAID**.

QTS starts to rebuild the RAID group.

Recovering a RAID group with a Degraded status

If one of more disks fail in a RAID group, but the number of disk failures is within the tolerance of the group's RAID type,then the following events occur:

- The statuses of the RAID group and its storage pool change to `Degraded`.
- Data on the RAID group and affected storage pool remains accessible.

1. Ensure you have one or more free disks in the NAS.
2. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
3. Select a storage pool or single static volume with the status `Degraded`.
4. Click **Manage**.
   The **Storage Pool Management** or **Volume Management** window opens.
5. Select a RAID group with the status `Degraded`.
6. Click **Manage**, and then select **Rebuild RAID Group**.
   The **Rebuild RAID Group** window opens.
7. Click **Rebuild**.
8. Select one or more disks.
   QTS displays the number of disks that you must select, according to the number of disk failures.
9. Click **Apply**.

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 **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 **Storage & Snapshots** > **Storage** > **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 group, the status of the group changes to `Scrubbing`.

Self-encrypting drives (SEDs)

A self-encrypting drive (SED) is a drive with encryption hardware built into the drive controller. SEDs automatically encrypt all data as it is written to the drive and decrypt all data as it is read from the drive. Data stored on SEDs are always fully encrypted by a data encryption key, which is stored on the drive's hardware and cannot be accessed by the host operating system or unauthorized users. The encryption key can also be encrypted by a user-specified encryption password that allows the SED to be locked and unlocked.

Because encryption and decryption are handled by the drive, accessing data on SEDs does not require any extra CPU resources from the host device. Data on SEDs also become inaccessible if the SEDs are physically stolen or lost. For these reasons, SEDs are widely preferred for storing sensitive information.

In QTS, you can use SEDs to create SED secure storage pools and SED secure static volumes. You can also use SEDs to create regular storage pools and volumes, but the self-encrypting function on the SEDs would be disabled.

SED types

QNAP categorizes SED types according to the industry-standard specifications defined by the Trusted Computing Group (TCG). Supported SED types are listed in the following table.

To check the SED type of an installed SED, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks** and click a SED.

SED Type	Supported
TCG Opal	Yes
TCG Enterprise	Yes (QTS 5.0.1 and later)
TCG Ruby	Yes (QTS 5.2.0 and later)

Creating a SED secure storage pool

1. Go to **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**, and then select **New Storage Pool**.

   The **Create Storage Pool Wizard** window opens.
3. Optional: Enable Qtier.
   Qtier is an automated-tiering storage solution that automatically moves frequently accessed data to high-performance drives for greater read and write performance, and infrequently accessed data to higher-capacity drives for more cost-effective storage. Once Qtier is enabled, it cannot be disabled. You can choose to enable Qtier later.
   For details, see Qtier.
4. Enable SED encryption and create a SED secure storage pool.
   You must have free SEDs on the NAS.
5. Click **Next**.

6. 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 becomes inaccessible until the expansion unit is reconnected.

7. Select one or more disks.

   Warning
   All data on the selected disks will be deleted.

8. If you enabled Qtier, click **OK**.

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

   Tip
   Use the default RAID type if you are unsure of which option to choose.
   For details, see RAID types.

10. 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 subgroups share the same spare disk.

    a. Identify the disk to use as a hot spare.

    b. Under **Mode**, click **Data**.

    c. Select **Spare**.

11. Optional: Select the number of RAID 50 or RAID 60 subgroups.
    The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.

    - A higher number of subgroups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
    - A lower number of subgroups 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 subgroups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

12. If you enabled Qtier, select disks for at least one more tier and configure the RAID type and optionally a spare disk for each tier.
    For details, see Qtier requirements.
13. Click **Next**.
14. 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 SSD Profiling Tool from App Center.
15. Optional: Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
16. Optional: Configure pool guaranteed snapshot space.
    Pool 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.
17. Specify the encryption password.

    Note
    The encryption password is used for locking and unlocking the SED secure storage pool, and is required for disabling SED security to change the SED pool into a standard pool without encryption.

    The encryption password must consist of 8 to 32 characters from any of the following groups:

    - Letters: A to Z, a to z
    - Numbers: 0 to 9
    - Special characters: Any except for space ( )

    Warning
    Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable.
18. Optional: Select **Auto unlock on startup**.
    This setting enables the system to automatically unlock and mount the SED pool whenever the NAS starts, without requiring the user to enter the encryption password.

    Warning
    Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

19. Click **Next**.
20. Verify the storage pool information.
21. Click **Create**.
    A confirmation message appears.

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

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

Creating a SED secure static volume

To create a regular static volume, see Creating a static volume.

1. Go to **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 becomes inaccessible until the expansion unit is reconnected.
6. Select **Create SED secure static volume**.
   The list of disks only displays SEDs.
7. Select one or more disks.
8. 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 **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 unsure of which option to choose.
For details, see RAID types.

9. 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 disk failure protection.

10. Optional: Select the number of RAID 50 or RAID 60 subgroups.
The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.

    - A higher number of subgroups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
    - A lower number of subgroups 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 subgroups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

11. Click **Next**.

12. 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
    - Special characters: Hyphen (-), underscore (_)
13. Configure the SED settings.
    a. Specify the encryption password.

    > **Note**
    > The encryption password is used for locking and unlocking the SED secure static volume, and is required for disabling SED security to change the SED volume into a standard volume without encryption.

    The password must contain 8 to 32 characters, with any combination of letters, numbers, and special characters. Spaces are not allowed.

    > **Warning**
    > Remember this password. If you forget the password, the volume will become inaccessible and all data will be unrecoverable.

    b. Verify the encryption password.
    c. Optional: Select **Auto unlock on startup**.
    This setting enables the system to automatically unlock and mount the SED volume whenever the NAS starts, without requiring the user to enter the encryption password.

    > **Warning**
    > Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

14. 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 SSD Profiling Tool from App Center.

15. 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.
Accelerate performance with SSD cache	QTS adds data from this volume to the SSD cache to improve read or write performance.	-
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the user account that creates the shared folder has read/write access to the folder.	• Specify a folder name. • Select **Create this folder as a snapshot shared folder**. A snapshot shared folder enables faster snapshot creation and restoration.
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.	Select a value.

16. Click **Next**.
17. 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.

SED storage pool and static volume actions

To perform the following actions, go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**, select a SED pool or volume, click **Manage**, then select **Actions** > **SED Settings**.

Action	Description
Change SED Pool Password Change SED Volume Password	Change the encryption password. **Warning** Remember this password. If you forget the password, the pool or volume will become inaccessible and all data will be unrecoverable. You can also enable **Auto unlock on startup**. This setting enables the system to automatically unlock and mount the SED pool or volume whenever the NAS starts, without requiring the user to enter the encryption password **Warning** Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.
Lock	Lock the pool or volume. All volumes, LUNs, snapshots, and data in the pool or volume will become inaccessible until it is unlocked.
Unlock	Unlock a locked SED pool or volume. All volumes, LUNs, snapshots, and data in the pool or volume will become accessible.
Disable SED Security	Remove the encryption password and disable the ability to lock and unlock the pool or volume. The SED pool/volume becomes a standard pool/volume without encryption.
Enable SED Security	Add an encryption password and enable the ability to lock and unlock the pool or volume. The standard pool/volume becomes a SED pool/volume with encryption enabled.

Removing a locked SED storage pool or static volume

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a locked SED storage pool or static volume.
3. Click **Manage**, and then click **Remove**.
   The **Removal Wizard** window opens.

4. Select a removal option.

Option	Description
Unlock and remove pool, data, and saved key	This option unlocks the SED disks in the storage pool or static volume, and then deletes all data. The storage pool or static volume is removed from the system. You must enter the encryption password.
Remove pool without unlocking it	This option removes the storage pool or static volume without unlocking the disks. The SED disks cannot be used again until you perform one of the following actions: • Unlock the disks. Go to **Disks/VJBOD**, click ⋮, and then select **Recover** > **Scan and Attach Storage Pool**. • Erase the disks using SED erase.

5. Click **Apply**.

The system removes the locked SED storage pool or static volume.

Erasing a disk using SED Erase

SED Erase erases all of the data on a locked or unlocked SED disk and removes the encryption password.

> **Note**
> If the disk is the only disk in use on the NAS, you must create another storage pool before you can erase the disk.

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.
2. Select a SED disk.
3. Click **Actions**, and then select **SED Erase**.
   The **SED Erase** window opens.
4. Enter the disk's Physical Security ID (PSID).

   > **Tip**
   > The PSID can usually be found on the disk label.
   > If you cannot find the PSID, contact the disk manufacturer.

5. Click **Apply**.

The system erases all data on the SED.

SED status

To view the encryption status of a SED, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks** and click an installed SED.

SED Status	Description
Uninitialized	The SED is uninitialized. Drive encryption is deactivated.
Unlocked	The SED is initialized and unlocked. Drive encryption is activated. Data on the SED is encrypted and accessible.
Locked	The SED is initialized and locked. Drive encryption is activated. Data on the SED is encrypted and inaccessible.
Blocked	The SED is blocked for security reasons. The drive cannot be initialized. **Note** To unblock the SED, reinsert the disk or erase the disk using **SED Erase**. For details, see Erasing a disk using SED Erase.

Expansion units

Expansion units are designed to expand the storage capacity of a QNAP NAS by adding extra drive bays. Expansion units can be connected to the NAS using USB, Mini-SAS, Thunderbolt, or other cable type.

Tip
Expansion units used to be known as JBODs.

Expansion unit actions

Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **NAS and Enclosure** and select an expansion unit to perform one of the following actions.

Action	Description
Enclosure Info	View full hardware details of the expansion unit, including the model, serial number, firmware version, BUS type, CPU temperature, system temperature, power status, and fan speeds.
Action > **Locate**	Prompt the expansion unit chassis LEDs to blink, so that you can locate the device in a server room or rack.

Action	Description
Action > **Safely Detach**	Stop all activity and safely unmount the enclosure from the host NAS.
Action > **Update Firmware**	Update the expansion unit's firmware.
Action > **Rename Enclosure**	Rename the selected expansion unit.
RAID Group	View details about each RAID group on the expansion unit, including its RAID type, capacity, and member disks.

Expansion unit recovery

If an expansion unit is accidentally disconnected from the NAS, for example by an unscheduled shutdown or disconnected cable, then the following changes to storage state will occur:

- The status of all storage pools on the expansion unit will change to `Error`.
- The status of all RAID groups on the expansion unit will change to `Not Active`.

If you encounter this situation, reconnect the expansion unit to the NAS and QTS will automatically guide you through the recovery process.

You can also perform recovery manually. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**, and then click ⋮ > **Recover** to perform one of the following actions.

Action	Description
Reinitialize enclosure ID	Reset all expansion unit IDs, and then give each unit a new ID number starting from 1 based on the order that they are physically connected. **Tip** Use this action if the expansion unit IDs appear out of sequential order in the enclosure list.
Attach and Recover Storage Pool	Scan all free disks on the NAS and all connected expansion units for existing volumes, LUNs, and storage pools. **Tip** Perform this action after moving disks between NAS devices.

QNAP external RAID devices

About QNAP external RAID devices

QNAP External RAID devices are a series of expansion units designed to increase the storage capacity of your NAS or computer. External RAID devices are different from other QNAP expansion units in that they feature hardware RAID. A host can either access the disks in an external RAID individually, or the external RAID device can combine the disks using hardware RAID so that the host accesses them as one large disk. Some external RAID devices have hardware switches for storage configuration, while other models can only be configured through a software interface.

QNAP external RAID device types

Device Type	Summary	Example Models
External RAID enclosure	An expansion unit featuring hardware RAID that connects to a NAS or computer using a connector cable.	TR-004, TR-002, TR-004U
Drive Adapter	A small enclosure featuring hardware RAID that allows you to install 1-2 smaller drives into a larger drive bay in a NAS or computer (e.g. two 2.5-inch SATA drives in a 3.5-inch bay).	QDA-A2AR, QDA-A2MAR, QDA-U2MP

Note
When an external RAID enclosure is connected to a QNAP NAS, you can only create one RAID group on the enclosure. All disks not in the RAID group are automatically assigned as spare disks, and cannot be used for storage until the RAID group has been deleted.

Storage modes

QNAP RAID enclosures support two different storage modes.

Important
QNAP drive adapters only support NAS storage mode.

Storage Mode	Description	Supported RAID Types	Supported Hosts
NAS Storage	Use the RAID enclosure's storage capacity to create a new storage pool or static volume on a QNAP NAS.	• JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10	QNAP NAS running QTS 4.3.6 or later
External Storage	Use the RAID enclosure as an external USB disk. This mode supports multiple RAID groups. Each RAID group appears as a separate disk when the enclosure is connected to a host.	• Individual • JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10	• Windows • macOS • Linux • QNAP NAS • Other NAS devices

Storage configuration

Creating a storage pool on a RAID enclosure

Important

- The Mode switch on the RAID enclosure must be set to Software Control mode. For details, see the enclosure's hardware user guide.
- The RAID enclosure must not contain any existing RAID groups.

Warning

To prevent errors or data loss, do not change the enclosure Mode switch from Software Control to any other mode while the enclosure is connected to the NAS.

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices**, and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Configure**.
   The **External RAID Device Configuration Wizard** opens.
4. Click **Next**.

5. Select two or more disks.

   Warning

   - All data on the selected disks will be deleted.
   - All unselected disks will be automatically assigned as spare disks, and cannot be used until the RAID group has been 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
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5
Four	JBOD, RAID 0, RAID 5, RAID 10	RAID 5

   Tip
   Use the default RAID type if you are unsure of which option to select.

7. Click **Next**.
8. Select **Create Storage Pool**.
9. Click **Create**.
   A confirmation message appears.
10. Click **OK**.
    - The RAID enclosure creates the RAID group.
    - The **Create Storage Pool Wizard** opens on the **Select Disks** screen.
    - The RAID group you created is automatically selected and the RAID type is set to `Single`.
11. Click **Next**.
12. Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
13. Configure pool guaranteed snapshot space.
    Pool 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.
14. Click **Next**.

15. Click **Create**.
    A confirmation message appears.
16. Click **OK**.

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

Creating a storage pool on a drive adapter

1. Set the drive adapter to the RAID mode that you want using the device's hardware Mode switch.
2. Install the drive adapter in the NAS.
   For details, see the drive adapter's hardware user guide.
3. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
4. Perform one of the following actions.
   - Click **New Storage Pool**.
   - Click **Create**, and then select **New Storage Pool**.

   The **Create Storage Pool Wizard** window opens.
5. Click **Next**.
6. Under **Enclosure Unit**, select **NAS Host**.
7. In the list of disks, select the drive adapter.
8. Under **RAID Type**, select **Single**.
9. Click **Next**.
10. 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 SSD Profiling Tool from App Center.
11. Optional: Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
12. Optional: Configure pool guaranteed snapshot space.
    Pool 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.
13. Click **Next**.

14. Click **OK**.
    - The **Create Storage Pool Wizard** opens on the **Select Disks** screen.
    - The RAID group created in steps 3-5 is selected as the disk for the storage pool.
    - The RAID type is set to `Single`.
15. Click **Next**.
16. Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
17. Click **Next**.
18. Click **Create**.
    A confirmation message appears.
19. Click **OK**.

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

Creating a static volume on a RAID enclosure

Important

- The Mode switch on the RAID enclosure must be set to Software Control mode. For details, see the enclosure's hardware user guide.
- The RAID enclosure must not contain any existing RAID groups.

Warning

To prevent errors or data loss, do not change the enclosure Mode switch from Software Control to any other mode while the enclosure is connected to the NAS.

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices**, and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Configure**.
   The **External RAID Device Configuration Wizard** opens.
4. Click **Next**.

5. Select two or more disks.

   Warning

   - All data on the selected disks will be deleted.
   - All unselected disks will be automatically assigned as spare disks, and cannot be used until the RAID group has been 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
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5
Four	JBOD, RAID 0, RAID 5, RAID 10	RAID 5

   Tip
   Use the default RAID type if you are unsure of which option to select.
   For details on RAID types, see RAID types.

7. Click **Next**.
8. Select **Create Volume**.
9. Click **Create**.
   A confirmation message appears.
10. Click **OK**.
    - The RAID enclosure creates the RAID group.
    - The **Volume Creation Wizard** opens on the **Select Disks** screen.
    - The RAID group you created is automatically selected and the RAID type is set to `Single`.
11. Click **Next**.
12. 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 (-), underscore (_)
13. Optional: Encrypt the volume.
    QTS encrypts all data on the volume with 256-bit AES encryption.

a. Specify an encryption password.
The password must contain 8 to 32 characters, with any combination of letters, numbers, and special characters. Spaces are not allowed.

> **Warning**
> If you forget the encryption password, all data will become inaccessible.

b. Verify the encryption password.

c. Optional: Select **Auto unlock on startup**.
This setting enables the system to automatically unlock and mount the encrypted volume whenever the NAS starts, without requiring the user to enter the encryption password or encryption key file.

> **Warning**
> Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

14. 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 SSD Profiling Tool from App Center.

15. 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.
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 user account that creates the shared folder has read/write access to the folder. **Note** This setting is only available when logged in as "admin".	**a.** Specify a folder name. **b.** Select **Create this folder as a snapshot shared folder**. A snapshot shared folder enables faster snapshot creation and restoration.
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.	Select a value.

16. Click **Next**.
17. Click **Finish**.
    A confirmation message appears.
18. Click **OK**.

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

Creating a static volume on a drive adapter

1. Set the drive adapter to the RAID mode that you want using the device's hardware Mode switch.
2. Install the drive adapter in the NAS.
   For details, see the drive adapter's hardware user guide.
3. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
4. 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.

5. Select **Static Volume**.
6. Click **Next**.
7. Under **Enclosure Unit**, select **NAS Host**.
8. In the list of disks, select the drive adapter.
9. Under **RAID Type**, select **Single**.
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 (-), underscore (_)
12. Optional: Encrypt the volume.
    QTS encrypts all data on the volume with 256-bit AES encryption.
    a. Specify an encryption password.
    The password must contain 8 to 32 characters, with any combination of letters, numbers, and special characters. Spaces are not allowed.

    Warning
    If you forget the encryption password, all data will become inaccessible.

    b. Verify the encryption password.
    c. Optional: Select **Auto unlock on startup**.
    This setting enables the system to automatically unlock and mount the encrypted volume whenever the NAS starts, without requiring the user to enter the encryption password or encryption key file.

    Warning
    Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.
13. 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 SSD Profiling Tool from App Center.

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.
Accelerate performance with SSD cache	QTS adds data from this volume to the SSD cache to improve read or write performance.	-
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the user account that creates the shared folder has read/write access to the folder. **Note** This setting is only available when logged in as "admin".	**a.** Specify a folder name. **b.** Select **Create this folder as a snapshot shared folder**. A snapshot shared folder enables faster snapshot creation and restoration.
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.	Select a value.

15. Click **Next**.
16. Click **Finish**.
    A confirmation message appears.
17. Click **OK**.

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

Configuring a RAID enclosure as an external storage device

Important

- The Mode switch on the RAID enclosure must be set to Software Control mode. For details, see the enclosure's hardware user guide.
- The RAID enclosure must not contain any existing RAID groups.

Warning
To prevent errors or data loss, do not change the enclosure Mode switch from Software Control to any other mode while the enclosure is connected to the NAS.

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices**, and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Configure**.
   The **External RAID Device Configuration Wizard** opens.
4. Click **Next**.
5. Select two or more disks.

   Warning
   - All data on the selected disks will be deleted.
   - All unselected disks will be automatically assigned as spare disks, and cannot be used until the RAID group has been 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
Two	JBOD, RAID 0, RAID 1	RAID 1
Three	JBOD, RAID 0, RAID 5	RAID 5
Four	JBOD, RAID 0, RAID 5, RAID 10	RAID 5

   Tip
   Use the default RAID type if you are unsure of which option to choose.
7. Click **Next**.
8. Select **Create External Storage Space**.
9. Click **Create**.
   A confirmation message appears.
10. Click **OK**.
11. Go to **Storage & Snapshots** > **Storage** > **External Storage**.

12. Select the uninitialized partition on the RAID enclosure.

    Tip
    Double-click on the RAID enclosure to see all of its partitions.

13. Click **Actions**, and then select **Format**.
    The **Format Partition** window opens.

14. Select a file system.

File System	Recommended Operating Systems and Devices
NTFS	Windows
HFS+	macOS
FAT32	Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets **Important** The maximum file size is 4 GB.
exFAT	Windows, macOS, some cameras, mobile phones, video game consoles, tablets **Important** Verify that your device is compatible with exFAT before selecting this option.
EXT3	Linux, NAS devices
EXT4	Linux, NAS devices

15. Specify a disk label.
    The label must consist of 1 to 16 characters from any of the following groups:

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

16. Optional: Enable encryption.

    a. Select an encryption type.
    Select one of the following options:

    - AES 128 bits

- AES 192 bits
- AES 256 bits

b. Specify an encryption password.
The password must consist of 8 to 16 characters from any of the following groups:

- Letters: A to Z, a to z
- Numbers: 0 to 9
- All special characters (excluding spaces)

c. Confirm the encryption password.

d. Optional: Select **Save encryption key**.
Select this option to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted external storage 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 external storage will become inaccessible and all data will be lost.

17. Click **Format**.
A warning message appears.
18. Click **OK**.

QTS formats the RAID group on the external RAID enclosure as an external disk. You can view and manage it at **Storage & Snapshots** > **Storage** > **External Storage**.

QTS external RAID management

Open **Storage & Snapshots**, click **External Storage Devices**, and then select **External Storage Device Management** to view, manage, and configure RAID devices connected to the NAS.

Warning
To prevent errors or data loss, do not change a RAID device's Mode switch from Software Control to any other mode while the device is connected to the NAS.

UI Element	Description
External storage device	Select a RAID device to manage.

UI Element	Description
Safely Detach	Disconnect a RAID device from the NAS when the device is in NAS Storage mode. QTS stops and then safely removes all storage pools, shared folders, volumes, and LUNs stored on the device, without deleting any data. You can then connect it to another NAS or computer. **Tip** To access the storage pools, shared folders, volumes, and LUNs on another QNAP NAS, connect the RAID device to the target NAS, go to **Storage & Snapshots** > **Disks/VJBOD**, click ⋮, and then select **Recover** > **Scan all Free Disks**. **Important** This button only appears when the device is in NAS Storage mode.
Eject	Safely disconnect a RAID device from the NAS when the device is in External Storage mode. You can then connect it to another NAS or computer. **Important** This button only appears when the device is in External Storage mode.
Configure	Create a RAID group on the RAID device and configure the storage mode. **Important** The RAID device's Mode switch must be set to Software Control mode.
Check for Update	Update the RAID device's firmware, either over the internet or from a local file. For details, see Manually updating external RAID device firmware in QTS.
Manage > **Configure Spare Disk**	Configure a global hot spare disk for the RAID device. If a disk in any RAID group on the device fails, the hot spare disk automatically replaces the faulty disk. For details, see Configuring a spare disk.
Manage > **Remove**	Delete the RAID group. The member disks are automatically assigned as global spare disks if the device contains any other RAID groups. **Warning** All data on the selected disks will be deleted.

UI Element	Description
Manage > **View Disks**	View the information about the disks installed in the RAID device, including their status and health information. **Note** Selecting this option takes you to the **Disks/VJBOD** screen.

Migrating an external RAID enclosure in NAS storage mode

Follow these steps to move a RAID enclosure containing a storage pool or static volume from a QNAP NAS to a different QNAP NAS (which we will call the target NAS).

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **NAS and Enclosure**.
2. Select an enclosure.
3. Select **Action** > **Safely Detach**.
   The **Safely Detaching Enclosure** window opens.
4. Click **Apply**.

   Warning
   Do not disconnect or power off the RAID enclosure until the enclosure has been detached.

   A confirmation message appears.
5. Disconnect the RAID enclosure from the NAS.
6. Connect the RAID enclosure to the target QNAP NAS.
7. On the target NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
8. Click ⋮ and select **Recover** > **Attach Storage Pool**.
   A confirmation message appears.
9. Click **OK**.
   QTS scans the RAID enclosure for storage pools and static volumes, and then displays them on the **Recover Wizard** window.
10. Click **Apply**.

QTS makes all storage pools, volumes, and LUNs on the RAID enclosure available on the target NAS at **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.

Manually updating external RAID device firmware in QTS

1. Open **Storage & Snapshots**.

2. Click **External Storage Devices** and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Select a RAID device.
4. Click **Check for Update**.
   The **Firmware Management** window opens. QTS checks online for the latest device firmware.
5. Select a firmware update method.

Firmware Update Method	Description
Install the latest firmware version	Download and install the latest version of the device firmware. **Note** You can only select this option if QTS has checked online and found a newer firmware version than the one currently installed on the device.
Select a local firmware file	Update the firmware using a local firmware IMG file on your computer. Click **Browse** to select the file. **Tip** You can download firmware updates at https://download.qnap.com.

6. Click **Update**.

   Warning
   Do not power off or disconnect the RAID device unless prompted.

7. Follow the instructions to install the firmware update.
   Depending on the model you may be asked to power off then power on the device, or disconnect then reconnect the device.
   QTS re-detects the device and displays a notification message.
8. Wait for confirmation that the firmware update has finished.
9. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
10. Click ⋮ and select **Recover** > **Scan and Attach Storage Pool**.

Configuring a spare disk

1. Open **Storage & Snapshots**.

2. Click **External Storage Devices** and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Manage**, and then select **Configure Spare Disk**.
   The **Configure Spare Disk** window opens.
4. Select one or more free disks.
5. Click **Apply**.

The selected disks are assigned as spare disks for the RAID group on the external RAID device.

External RAID device health

To view the status and health of RAID enclosures connected to the NAS, or drive adapters and the disks installed in them, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.

The Autoplay menu

The Autoplay menu opens when you connect a RAID enclosure to a NAS. The actions available in this menu vary depending on the enclosure's current storage mode and RAID configuration.

Action	Description
Open and view files	Opens the enclosure in **File Station**.
Use this device for backup	Opens **HBS**.
Configure external storage partitions	Opens **Storage & Snapshots** > **Storage** > **External Storage**. For more information, see Configuring a RAID enclosure as an external storage device.
Create NAS storage space	Opens **Storage & Snapshots** > **Storage** > **Storage/Snapshots**. For more information, see Creating a storage pool on a RAID enclosure.
Edit access permissions	Opens the **Edit Shared Folder Permissions** window to edit access permissions for this device.

QNAP JBOD enclosures

About QNAP JBOD enclosures

QNAP JBOD enclosures are a series of expansion units designed to increase the storage capacity of your NAS, computer, or server. JBOD enclosures offer a wide range of storage applications. You can manage drives independently or group them together in a software RAID configuration using a host NAS, computer, or server. QNAP offers JBOD enclosures with USB 3.2 Gen 2 Type-C or SFF interface ports to ensure quick and efficient data transfer between the JBOD enclosure and the host device.

QNAP JBOD enclosure types

Enclosure Type	Description	Supported Platforms	Example Models
Single-controller SAS JBOD enclosure	A JBOD enclosure that uses SFF interface ports to connect to a NAS or server. These enclosures can only connect to a host device with an installed PCIe SAS storage expansion card.	• Server: Windows, Linux • NAS: QTS, QuTS hero	TL-R1220Sep-RP, TL-R1620Sep-RP
Dual-controller SAS JBOD enclosure	A JBOD enclosure with dual controllers that uses SFF interface ports to connect to a NAS or server. These enclosures can only connect to a host device with available Mini-SAS ports or an installed PCIe SAS storage expansion card.	• Server: Windows, Linux • NAS: QES	TL-R1620Sdc
SATA JBOD enclosure	A JBOD enclosure that uses SFF interface ports to connect to a NAS or computer. These enclosures can only connect to a host device with an installed QNAP QXP host bus adapter.	• Computer: Windows, Linux • NAS: QTS, QuTS hero	TL-D400S, TL-R1200S-RP
USB JBOD enclosure	A JBOD enclosure that uses USB 3.2 Gen 2 Type-C ports to connect to a NAS or computer.	• Computer: Windows, Linux, macOS • NAS: QTS, QuTS hero	TL-D800C, TL-R1200C-RP

QTS JBOD management

You can manage JBOD enclosures in QTS from the following locations in the Storage & Snapshots utility.

Location	Description
Disks/VJBOD	View, manage, and configure storage for attached JBOD enclosures. You can create storage pools, volumes, and RAID groups using disks installed in the JBOD enclosure.

Location	Description
External Storage	View and manage attached non-SAS JBOD enclosures and installed disks.
Topology	View and manage attached SAS JBOD enclosures.

Updating JBOD enclosure firmware in QTS

1. Open **Storage & Snapshots**.
   QTS periodically checks for the latest firmware for each connected enclosure on login. If a new firmware update is available, QTS opens the **Start Firmware Update** window.
2. Follow the instructions to install the firmware update.
   Depending on the model you may be asked to power off then power on the device, or disconnect then reconnect the device.
   QTS re-detects the device and displays a notification message.
3. Wait for confirmation that the firmware update has finished.
4. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
5. Click ⋮ and select **Recover** > **Scan and Attach Storage Pool**.

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, offering performance similar to having 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
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 4 GB of installed memory. Using Qtier with less than 4 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	-
Three tiers	Ultra-high speed	High speed	Capacity

Disk Requirements

Qtier Disk Types

Disk Type	Ultra-High Speed Tier	High Speed Tier	Capacity Tier
PCIe/NVMe SSD	Supported	-	-
SAS SSD	Supported	Supported	-
SATA SSD	Supported	Supported	-
SAS HDD	-	Supported	Supported
NL-SAS HDD	-	-	Supported
SATA HDD	-	-	Supported

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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Perform one of the following actions.

Current NAS State	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. Enable Qtier.
4. Optional: Enable SED encryption and create a SED secure storage pool.
   You must have free SEDs on the NAS.
   For details, see Self-encrypting drives (SEDs).
5. Click **Next**.
6. Configure a tier.
   a. 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 becomes inaccessible until the expansion unit is reconnected.

   b. Select one or more disks.

      Warning
      All data on the selected disks will be deleted.

Important

- For data safety, you cannot select disks that have the status `Warning`.
- The status `In Use` means that a disk is currently formatted as an external disk, and may contain current user data.
- If you select a disk with the status `In Use`, QTS will temporarily stop all disk storage services on the NAS in order to unmount the disk, and then delete all data and partitions on the disk.
- The number of disks you can select depends on the RAID type you want to select. For details, see the following:
  - RAID types
  - QNAP RAID Calculator
- If you select multiples of three disks and select Triple Mirror for the RAID type, every three disks will form an individual RAID group in the storage pool. You can select a maximum of 15 disks with Triple Mirror.

c. Click **OK**.

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

Tip
Use the default RAID type if you are unsure of which option to choose. For details, see RAID types.

e. 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 subgroups share the same spare disk.

Tip
Under **Role**, click **Data** and then select **Spare**.

f. Select the number of RAID 50 or RAID 60 subgroups.
The selected disks are divided evenly into the specified number of RAID 5 or 6 groups.

- A higher number of subgroups results in faster RAID rebuilding, increased disk failure tolerance, and better performance if all the disks are SSDs.
- A lower number of subgroups 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 subgroups of 3 disks, 3 disks, and 4 disks will provide only 9 disks of storage capacity.

7. Repeat the previous steps to configure at least one more tier.
   For details, see Qtier requirements.
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 SSD Profiling Tool from App Center.

10. Optional: Configure the alert threshold.
    QTS issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
11. Optional: Configure pool guaranteed snapshot space.
    Pool 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.
12. If you enabled SED encryption, configure the SED settings.

    a. Specify the encryption password.
       The encryption password must consist of 8 to 32 characters from any of the following groups:

       - Letters: A to Z, a to z
       - Numbers: 0 to 9
       - Special characters: Any except for space ( )

       > **Warning**
       > Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable.

    b. Optional: Select **Auto unlock on startup**.
       This setting enables the system to automatically unlock and mount the SED pool whenever the NAS starts, without requiring the user to enter the encryption password.

> **Warning**
> Enabling this setting can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

13. Click **Next**.
14. Verify the storage pool information.
15. Click **Create**.
    A confirmation message appears.

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

16. 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Select **Action** > **Upgrade to Qtier**.
   The **Upgrade to Qtier Pool Wizard** window opens.
5. Create a second tier.
   a. Click SSD, SAS, or SATA.
   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 SSD, SAS, or SATA.
   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 SSD Profiling Tool 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

To manage Qtier on a storage pool, go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**. Select a Qtier storage pool, click **Manage**, and then click **Qtier Auto Tiering**.

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.

Item	Description
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 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 `Processing`.

Qtier statistics

The appearance and functionality of Qtier depends on the current tiering schedule. To view Qtier statistics on a storage pool, go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**. Select a Qtier storage pool, click **Manage**, and then click **Statistics**.

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.

Configuring the 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.

1. Go to **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**.

Removing the ultra-high speed tier

Removing the ultra-high speed tier converts a Qtier storage pool into a regular storage pool.

Important
You can only remove the ultra-high speed tier if the allocated storage pool space is less than the remaining storage pool capacity (Total storage pool capacity - Ultra-high speed tier capacity = Remaining capacity).

Tip
This feature is useful in the following situations:

- You want to use the SSD drives for another purpose.
- You want to increase the amount of SSD over-provisioning in the ultra-high speed tier.
- You want to change the RAID configuration of the ultra-high speed tier.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a Qtier storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Remove** and then select **Remove Ultra-High Speed Tier**.
   The **Ultra-High Speed Tier Removal Wizard** window opens.
5. Click **Next**.
6. Confirm that you want to remove the remove ultra-high speed tier.

7. Click **Next**.

   Warning
   The storage pool will be inaccessible while QTS removes the ultra-high speed tier. This process might take a long time.

8. Click **Finish**.

QTS creates a background task. The status of the storage pool changes to `Removing SSD Tier...`.

Configuring 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.

1. Go to **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.
- Encrypted shared folders do not support snapshots. Although you can take a snapshot of a volume containing encrypted shared folders and restore the volume with the encrypted shared folders intact, you cannot individually restore an encrypted shared folder from a snapshot. Encrypted shared folders in a snapshot also do not appear in the snapshot directory (@Recently-Snapshot).

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 **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. Click **Snapshot** and then select **Take a Snapshot**.
   The **Take a Snapshot** window opens.

4. Optional: Specify a name.

5. Optional: Choose to keep the snapshot permanently.
   If selected, QTS retains the snapshot indefinitely. If not selected, QTS may delete the snapshot according to the snapshot retention policy set for the volume or LUN.
   For more information, see Configuring a snapshot retention policy.

6. Select the LUN snapshot type.
   This setting is only available when taking a snapshot of a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the LUN.
Application consistent	The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QTS takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot. **Important** This option is only available for VMware vCenter, or for Volume Shadow Copy Service (VSS) aware applications running on a Windows server. You must install QNAP Snapshot Agent on the iSCSI initiator.

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

Tip
You can configure a separate snapshot schedule for each volume and LUN.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick volume, thin volume, or block-based LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Click **Schedule Snapshot**.
   The **Snapshot Settings** window opens.
5. Select **Enable schedule**.
6. Specify how often QTS will take a snapshot.
7. Select the LUN snapshot type.
   This setting is only available when taking a snapshot of a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the LUN.
Application consistent	The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QTS takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot. **Important** This option is only available for VMware vCenter, or for Volume Shadow Copy Service (VSS) aware applications running on a Windows server. You must install QNAP Snapshot Agent on the iSCSI initiator.

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 a snapshot retention policy

The snapshot retention policy determines how long QTS keeps each snapshot of a volume or LUN before deleting it. Each volume and LUN has its own individual snapshot retention policy.

Note
The snapshot retention policy does not apply to or count permanent snapshots.

Important
After you create or modify a snapshot retention policy, QTS applies the new policy to existing snapshots. If the new policy is more restrictive than the previous policy, for example changing from `Keep for: 5 days` to `Keep for: 2 days`, then QTS deletes existing snapshots to conform with the new policy.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick volume, thin volume, or LUN.
3. Click **Snapshot** and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Click **Schedule Snapshot**.
   The **Snapshot Settings** window opens.
5. Click **Snapshot Retention**.
6. Select a snapshot retention policy.

Snapshot Retention Policy	Description
Maximum amount of time to keep	Keep each snapshot for the specified length of time.
Maximum number of snapshots to keep	Keep a fixed maximum number of snapshots on the NAS. After the maximum number is reached, QTS deletes the oldest snapshot when taking a new snapshot.

Snapshot Retention Policy	Description
Smart Versioning	Take periodic snapshots and keep the specified maximum number of snapshots for the specified frequency. Once the specified number is reached, each new snapshot replaces the oldest snapshot of the specified frequency. Examples: • **Hourly**: 24 - The system takes a snapshot at the end of every hour. After the 24th hourly snapshot, the next hourly snapshot replaces the oldest hourly snapshot. • **Daily**: 7 - The system takes a snapshot at the end of every day. After the 7th daily snapshot, the next daily snapshot replaces the oldest daily snapshot. • **Weekly**: 4 - The system takes a snapshot at the end of every week. After 4th weekly snapshot, the next weekly snapshot replaces the oldest weekly snapshot. • **Monthly**: 12 - The system takes a snapshot at the end of every month. After the 12th monthly snapshot, the next monthly snapshot replaces the oldest monthly snapshot. **Important** The maximum number of snapshots for all frequencies combined is 256.

7. Click **OK**.

Configuring pool guaranteed snapshot space

Pool 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.

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick volume, thin volume, or LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.

4. Click **Pool Guaranteed Snapshot Space**, and then select **Configure**.
5. Enable **Enable Pool 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**.

Calculating snapshot size

You can calculate the number of snapshots and their total size in a volume or LUN over a specified period of time and view the result in chart form. When storage space is running low, this can help you determine how much space you can free up by deleting certain snapshots. The information can also help you adjust your snapshot settings to optimize your storage usage.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick volume, thin volume, or block-based LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Click **Calculate Size**.
   The **Snapshot Size Calculation** window opens.
5. Select a time range.
6. Click **Calculate**.
   The window displays a chart with information on the number of snapshots and their total size over the specified time range.
   You can adjust the time unit on the x-axis.

Deleting snapshots

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick volume, thin volume, or block-based LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Optional: Click ☰ to change to 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.
   The volume must contain at least one snapshot.
3. Click **Snapshot**, and then select **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**	Restore the files or folders to their original storage location. If the files or folders still exists on the NAS, then they will be overwritten with the older versions. **Warning** All changes made after the snapshot was taken will be deleted.
Select **Restore** > **Restore Files to**	Choose one of the following restoration options. • Restore the files or folders to a different location on the NAS. • Restore the files or folders to remote mounted storage space. • Restore a single shared folder as a new shared folder.

Action	Description
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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.

   Important
   The volume must have at least one snapshot.

3. Click **Snapshot**, and then select **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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.

2. Select a block-based LUN.

   Important
   The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **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 to data since the snapshot was taken 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

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

Important

- You must be using Windows 7, Windows 8 or Windows 10.
- The files must be stored on a thick volume or thin volume that has at least one snapshot.
- **Enable Windows Previous Versions** must be enabled in the shared folder settings.
- **Allow symbolic links between different shared folders** must be enabled at **Control Panel** > **Network & File Services** > **Win/Mac/NFS** > **Microsoft Networking** > **Advanced Options**.

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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.

   Important
   The volume must have at least one snapshot.

3. Click **Snapshot**, and then select **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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a block-based LUN.

   Important
   The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **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	Yes	Yes	Yes
Ransomware	Yes	Yes	Yes

Protects Against	Snapshots only	Snapshots + Local Snapshot Replica	Snapshots + Remote Snapshot Replica
RAID Group Failure • Member disks fail • Member disks are removed from the NAS	No	Yes	Yes
Storage Pool Failure • One or more RAID groups in the pool fail • Pool is deleted	No	Yes	Yes
NAS Hardware Failure • NAS cannot power on • QTS encounters an error and cannot start • NAS is stolen	No	No	Yes

Snapshot Replica requirements

NAS	Requirement
Source and Destination NAS	Must be a QNAP NAS that supports snapshots.
Source and Destination NAS	Both source and destination NAS devices must be running QTS. Replicating snapshots from QTS to QuTS hero or vice versa is not supported.
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.

NAS	Requirement
Destination NAS	**Allow SSH connections** must be enabled at **Control Panel** > **Network & File Services** > **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 **Storage & Snapshots** > **Data Protection** > **Snapshot Replica**.
2. Click **Create a Replication Job**.
   The **Create a Snapshot Replication Job** wizard opens.
3. Optional: Specify a job name.
4. Click **Next**.
5. Select the source volume or LUN.
6. Specify the address of the destination NAS.
   Perform one of the following actions.

Action	Destination NAS Location	Description
Manually specify the NAS address	LAN, WAN, Internet	Allows you to enter an IP address, hostname, or FQDN
Click **Detect** and then select a NAS from the list	LAN	Displays a list of all QNAP NAS devices on the local network
Click **Local Host**	Local NAS	Replicates snapshots between different storage pools on the same NAS

7. Specify an administrator account and password of the destination NAS.

   Important
   For security reasons, QNAP does not recommend using the "admin" account.

8. Optional: Specify a port.

   Tip
   The default port is 22.

9. Click **Test**.

   Important
   If prompted, complete 2-step verification. This is required if the destination NAS has enabled 2-step verification.

   QTS connects to the destination NAS using the specified administrator password, and checks that there is sufficient storage space.

10. Click **Next**.
11. Select the destination storage pool.
12. Click **Next**.
13. Select a backup plan.

Backup Plan	Description
Run each time after a local snapshot is taken	The replica job runs each time QTS creates the specified number of snapshots (the default value is 1). These snapshots can be created manually or on a schedule.
Run on a schedule	The replica job runs according to the specified schedule, and replicates all snapshots created since it was last run. If no new snapshots were created, it will not replicate any data. **Note** If you select **Take a new snapshot according to schedule and only replicate the new snapshot**, the system takes a snapshot before each scheduled job run and only replicates the new snapshot. If deselected, no new snapshots are automatically taken and all snapshots awaiting replication are replicated according to schedule. Choose one of the following scheduling options, and then click **Add**. • **Run on a schedule**: The job automatically runs daily, weekly, or monthly according to the specified settings. • **Run once**: The job runs once on a specific time and day.
Manual backup	The job does not run unless a user starts it.

14. Specify how many replicated snapshots to retain on the destination NAS.
    After the specified number is reached, QTS deletes the oldest snapshot each time it replicates a new snapshot.
15. Click **Next**.

16. Optional: Configure transfer settings.

Setting	Description
Encrypt transfer	QTS encrypts the snapshot before replicating it. • SSH connections must be allowed on the destination NAS. • The job must be run by an administrator account. • The port used by this job must be the same as the SSH port on the destination NAS.
Compress transfer	QTS compresses 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	Limits how much network bandwidth this job uses

17. Optional: 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 imports the source data when the job is next run.
    a. Connect an external storage device to the NAS.
    b. Select **Export source data to external storage device on first run**.
    c. Select the external storage device.
    d. Optional: Select **Skip the export** if you have already exported the source data to the external storage device.
18. Click **Next**.
19. Optional: Select **Execute backup immediately**.
When enabled, the job runs immediately after being created.
20. Review the job information.
21. Click **Finish**.
QTS creates the job.
22. Optional: If you chose to export source data to an external storage device, disconnect the storage device from the source NAS and connect it to the destination NAS.

Snapshot Replica management

To manage snapshot replica jobs and settings, go to **Storage & Snapshots** > **Data Protection** > **Snapshot Replica**.

Snapshot Replica job actions

Action	User Action
Enable the schedule	Click .
Disable the schedule	Click .
Start	Click .
Stop	Click .
Revert the snapshot	Click **Revert**.
Edit settings	Click and select **Edit**.
View logs	Click and select **Log**.
Delete	Click and select **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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.

   Important
   The volume must be the source volume for a Snapshot Replica job.

3. Click **Snapshot**, and then select **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**	Restore the files or folders to their original storage location. If the files or folders still exists on the NAS, then they will be overwritten with the older versions. **Warning** All changes made after the snapshot was taken will be deleted.
Select **Restore** > **Restore Files to**	Choose one of the following restoration options. • Restore the files or folders to a different location on the NAS. • Restore the files or folders to remote mounted storage space. • Restore a single shared 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.

   Important
   The volume must be the source volume for a Snapshot Replica job.

3. Click **Snapshot**, and then select **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 to data since the snapshot was taken 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 **Remote Revert**.
   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 shared folder or LUN to the state at which the snapshot was taken. Restoring data using snapshot revert is 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a block-based LUN.

   Important
   The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **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 to data since the snapshot was taken are not permanently lost.
Enable encryption during transfer	QTS encrypts the snapshot before sending it for additional security.
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 LUN 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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a thick or thin volume.

   > **Important**
   > The volume must have at least one snapshot.

3. Click **Snapshot**, and then select **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 **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Select a block-based LUN.

   > **Important**
   > The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **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 **Storage & Snapshots** > **Data Protection** > **Snapshot Vault**. Each replica job has its own separate vault.

Restoring files and folders from a snapshot vault

1. Go to **Storage & Snapshots** > **Data Protection** > **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 volume's 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 **Storage & Snapshots** > **Data Protection** > **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 volume's 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 **Storage & Snapshots** > **Data Protection** > **Snapshot Vault**.
2. Select a storage pool.
3. On a vault, click  .
   The **Snapshot Vault** 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.

Cache acceleration

Cache acceleration enables you to create an SSD cache to improve the read and write performance of the NAS.

Cache acceleration requirements

- The NAS model must support cache acceleration.
  For information about NAS and drive bay compatibility, see https://www.qnap.com/solution/ssd-cache.
- The NAS must have one or more free SSDs installed in a compatible drive bay.
- The NAS must have a suitable amount of installed memory.
  The amount of memory required depends on the size of the SSD cache.

SSD Cache Size	Required Memory	
	QTS 4.5.x (and earlier)	QTS 5.0.0 (and later)
512 GB	≧ 1 GB	-
1 TB	≧ 4 GB	≧ 2 GB
2 TB	≧ 8 GB	-
4 TB	≧ 16 GB	≧ 4 GB
8 TB	-	≧ 8 GB (ARM CPU)
16 TB	-	≧ 8 GB (x86 CPU)

Note
ARM-based NAS running QTS 4.5.x (or earlier) are limited to an SSD cache size of 1 TB.

Creating the SSD cache

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration**.
2. Click +.
   The **Create SSD Cache** window opens.

3. Click **Next**.
4. Select one or more SSDs.

   Warning
   All data on the selected disks will be deleted.

5. Select a cache type.

Cache Type	Description
Read-only	When data is read from a LUN or volume, QTS copies the data to the SSD cache to speed up future read requests.
Write-only	QTS writes incoming data to the SSD cache first, then flushes the data to regular storage later. Read access to the new data is also accelerated while it is in the cache.
Read-write	QTS uses the SSD cache for both read and write caching, accelerating both read and write speeds.

6. Select a RAID type.

   Warning
   Selecting a RAID type with no disk failure protection (Single, JBOD, RAID 0) when the cache type is `Write-only` or `Read-write` may result in data loss.

   Tip
   RAID 10 provides the best write cache performance.

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 SSD Profiling Tool from App Center.
   For details, see SSD Profiling Tool.

9. Select a cache mode.

Cache Mode	Description	Recommended Use Cases
Random I/O	Only small data blocks are added to the SSD cache. Larger blocks are accessed directly from regular storage.	Virtualization, databases
All I/O	Small and large data blocks are added to the SSD cache. Both sequential and random I/O requests are accelerated.	Video streaming, large file access operations

Tip
An HDD RAID group may outperform a SSD RAID group for sequential I/O if the ratio of HDDs to SSDs is 3:1 or greater, and the HDD group has a RAID type of RAID 0, 5, 6, or 10. However, SSDs will always be faster for random I/O. If the NAS contains a RAID group of type RAID 0, 5, 6, or 10 that contains three times more disks than the SSD cache, you should select **Random I/O**.

10. Optional: Configure the following advanced settings.

Setting	Description
Bypass block size	This value determines the maximum size of the data blocks that are stored in the SSD cache. Selecting a larger size may improve the cache's hit rate but uses more cache space. The default value is 1 MB.

11. Click **Next**.
12. Select which volumes and LUNs can use the SSD cache.

Important
For data safety, volumes and LUNs created on an external storage device cannot use the SSD cache if the cache type is `Read-write`.

13. Click **Next**.
14. Click **Create**.
    A confirmation message appears.
15. Select **I understand** and then click **OK**.

Expanding the SSD cache

The SSD cache can be expanded by adding a new SSD RAID group.

Important
Expanding the SSD cache clears all cached data.

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration**.
2. Click **Manage** and then select **Expand**.
   A confirmation message appears.
3. Click **OK**.
4. Select one or more SSDs.

   Warning
   All data on the selected disks will be deleted.
5. Select a RAID type.

   Warning
   Selecting a RAID type with no disk failure protection (Single, JBOD, RAID 0) when the cache type is `Write-only` or `Read-write` may result in data loss.

   Tip
   RAID 10 provides the best write cache performance.
6. Click **Expand**.
   A confirmation message appears.
7. Click **OK**.

Configuring SSD cache settings

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration**.
2. Click **Manage** and then select **Settings**.
   The **Switch SSD Cache** window opens.
3. Select which volumes and LUNs can use the SSD cache.

   Important
   For data safety, volumes and LUNs created on an external storage device cannot use the SSD cache if the cache type is `Read-write`.
4. Click **Next**.

5. Select a cache mode.

Cache Mode	Description	Recommended Use Cases
Random I/O	Only small data blocks are added to the SSD cache. Larger blocks are accessed directly from regular storage.	Virtualization, databases
All I/O	Small and large data blocks are added to the SSD cache. Both sequential and random I/O requests are accelerated.	Video streaming, large file access operations

Tip
An HDD RAID group may outperform a SSD RAID group for sequential I/O if the ratio of HDDs to SSDs is 3:1 or greater, and the HDD group has a RAID type of RAID 0, 5, 6, or 10. However, SSDs will always be faster for random I/O. If the NAS contains a RAID group of type RAID 0, 5, 6, or 10 that contains three times more disks than the SSD cache, you should select **Random I/O**.

6. Optional: Configure bypass block size.
This value determines the maximum size of the data blocks that are stored in the SSD cache. Selecting a larger size may improve the cache's hit rate but uses more cache space. The default value is 1 MB.
7. Click **Finish**.

Cache missing

If the write-only or read-write cache disks become unavailable because of hardware failure or physical removal from the NAS, all volumes using the write-cache will also become unavailable and will have `Cache Missing` as their status. QTS restricts access to these volumes to protect data integrity, as some volume data may be stored in the write cache without being flushed to disk.

When the SSD cache is missing, restore it using one of the following methods:

- If the SSD cache disks were removed from the NAS, re-insert the disks into the same drive bays.
- Resolve any RAID errors.
- Restart the NAS.

Removing a missing SSD cache

Important
You should only delete a missing SSD cache if it is not possible to restore the cache, for example, because of disk failure.

Warning
Removing a missing SSD write-only or read-write cache will delete all unflushed write data.

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration**.
2. Select **Manage** > **Remove**.
   A confirmation message appears.
3. Enter the admin password.
4. Click **OK**.
5. Restart the NAS.
6. Run a file system check on all volumes that used the SSD cache.
   For the details, see Volume file system check.

Removing the SSD cache

Warning
Removing an SSD from the SSD cache while write caching is enabled may cause data loss.

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration**.
2. Click **Manage** and then select **Remove**.
   A confirmation message appears.
3. Click **OK**.

QTS flushes all data in the cache to disk, then deletes the RAID groups. This process may take a long time.

External storage

QTS supports external USB and eSATA storage devices, such as flash drives, portable hard drives, and storage enclosures. After connecting a USB or eSATA external storage device to the NAS, the device and all of its readable partitions will be displayed in **Storage & Snapshots** > **Storage** > **External Storage**. QTS will also create a shared folder for each readable partition on the device.

External storage device actions

Action	Description
Erase	Delete all data and partitions on the device.
Eject	Safely unmount the external storage device from the NAS, so that you can disconnect it.

External storage partition actions

Action	Description
Storage Information	Display details about the selected partition, including partition name, capacity, used space, and file system type.
Format	Format the partition. For details, see Formatting an external storage disk or partition.
Encryption Management	Manage encryption on a previously encrypted device. You can lock or unlock the device, change the encryption password, or download the encryption key.
Eject	Unmount the partition. The external storage device and any stored partitions will continue working.

Formatting an external storage disk or partition

1. Go to **Storage & Snapshots** > **Storage** > **External Storage**.
2. Select a disk or partition.
3. Click **Actions**, and then select **Full Disk Format** or **Format**.
   The **Full Disk Format** or **Format Partition** window opens.
4. Select a file system.

File System	Recommended Operating Systems and Devices
NTFS	Windows
HFS+	macOS
FAT32	Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets **Important** The maximum file size is 4 GB.

File System	Recommended Operating Systems and Devices
exFAT	Windows, macOS, some cameras, mobile phones, video game consoles, tablets **Important** Verify that your device is compatible with exFAT before selecting this option.
EXT3	Linux, NAS devices
EXT4	Linux, NAS devices

5. Specify a label.
   The label must consist of 1 to 16 characters from any of the following groups:
   - Letters: A to Z, a to z
   - Numbers: 0 to 9
   - Special characters: Hyphen "-"
6. Optional: Enable encryption.
   a. Select an encryption type.
      Select one of the following options:
      - AES 128 bits
      - AES 192 bits
      - AES 256 bits
   b. Specify an encryption password.
      The password must consist of 8 to 16 characters from any of the following groups:
      - Letters: A to Z, a to z
      - Numbers: 0 to 9
      - All special characters (excluding spaces)
   c. Confirm the encryption password.
   d. Optional: Select **Save encryption key**.
      Select this option to save a local copy of the encryption key on the NAS. This enables the system to automatically unlock and mount the encrypted storage space 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 storage space will become inaccessible and all data will be lost.

7. Click **Format**.
   A warning message appears.
8. Click **OK**.

Remote disk

Remote disk enables QTS to act as an iSCSI initiator, allowing you to expand NAS storage by adding iSCSI LUNs from other NAS or storage servers as remote disks. When connected, remote disks are automatically shared on the **Shared Folders** screen. If a remote disk is disconnected, the disk will become inaccessible and QTS will try to reconnect to the target after 2 minutes. If the target cannot be reached, the status of the remote disk will change to `Disconnected`.

This feature is only available on NAS models that support iSCSI.

Remote disk limitations

Limit	Value
Maximum number of remote disks per NAS	8
Supported file systems	ext3, ext4, FAT32, NTFS, HFS+
Maximum remote disk size	16 TB

Adding a remote disk

1. Go to **Storage & Snapshots** > **Storage** > **Remote Disk**.
2. Click **Add Virtual Disk**.
3. Specify the IP address or hostname of the remote server.
4. Optional: Specify the iSCSI port of the remote server.
5. Click **Get Remote Disk**.
   QTS connects to the remote server and then lists all available iSCSI targets.
6. Select an iSCSI target.
7. Optional: Specify a CHAP username and password.
   This is required if the remote server has CHAP authentication enabled.

8. Optional: Enable CRC checksums.
   Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

9. Click **Next**.
10. Optional: Specify a disk name.
    The name must consist of 1 to 50 characters from the following groups:
    - Letters: a to z, A to Z
    - Numbers: 0-9
    - Special characters: space ( ), hyphen (-), underscore (_), period (.)

    The following are not allowed:
    - The last character is a space
    - The name starts with "_sn_"
11. Select a LUN.
12. Optional: Format the disk.
    Select one of the following options.

File System	Compatible Operating Systems and Devices
ext4	Linux, NAS devices
ext3	Linux, NAS devices
FAT32	Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets **Important** The maximum file size is 4 GB.
NTFS	Windows
HFS+	macOS

Warning
All data on the LUN will be deleted.

13. Configure synchronous I/O.
    If the remote server is using ZFS, select the ZFS Intent Log I/O mode for the LUN to improve data consistency or performance.

Mode	Description
Synchronous	All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a small impact on performance.
Asynchronous	All I/O transactions are treated as asynchronous. This option gives the highest performance, but has a higher risk of data loss in the event of a power outage. Ensure that a UPS (uninterrupted power supply) is installed when using this option.

14. Click **Next**.
15. Click **Finish**.

QTS adds the remote disk and shares it at **Control Panel** > **Privilege** > **Shared Folders**. By default only the admin account has access.

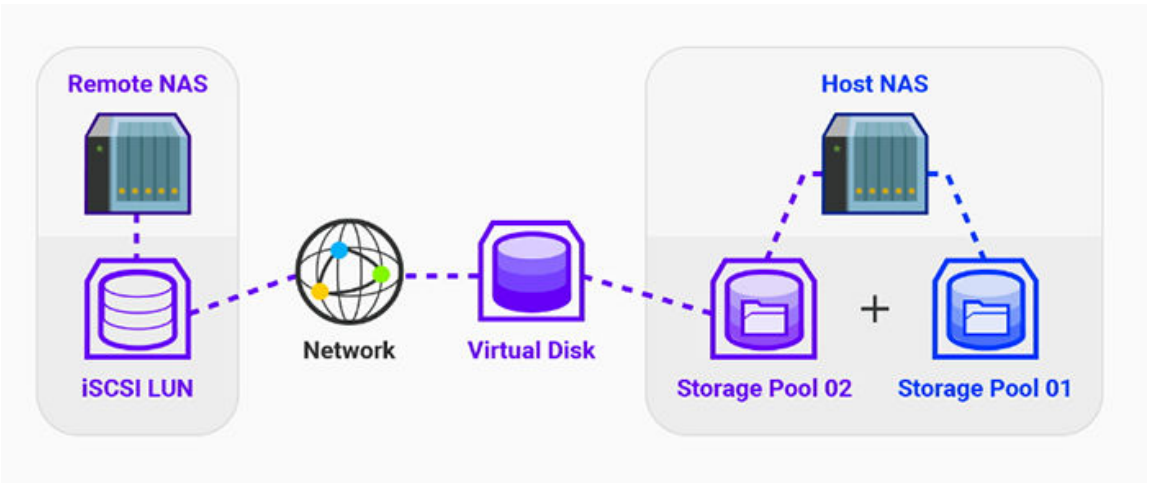
Remote disk actions

Action	Description
Edit	Edit the name of the disk.
Delete	Disconnect the remote disk and delete its shared folder. Existing data on the disk will not be deleted.

Action	Description
Format	Format the remote disk. Select one of the following file system options: • ext4 • ext3 • FAT32 • NTFS • HFS+ Select one of the following I/O options: • Synchronous • Asynchronous

VJBOD (Virtual JBOD)

VJBOD (Virtual JBOD) enables you to add storage space from other QNAP NAS devices to your NAS as local VJBOD disks, to create a virtual expansion enclosure. VJBOD disks can be used to create new local storage space, expanding local NAS storage capacity. VJBOD is based on iSCSI technology.



VJBOD requirements

Local NAS requirements:

- The NAS is running QTS 4.2.2 or later, or QuTS hero 4.5.0 or later.
- The NAS model supports VJBOD.
  For a list of supported series and models, see https://www.qnap.com/solution/vjbod.

Remote NAS requirements:

- The NAS is running QTS 4.2.1 or later, or QuTS hero.
- The NAS model supports iSCSI and storage pools.
- The NAS has a storage pool with at least 154 GB of free space, or an unused thick LUN with a capacity of 154 GB or more.

Tip

For a stable VJBOD connection, ensure the following conditions:

- All NAS devices are on the same local network.
- All NAS devices are configured with static IP addresses.
- On a remote NAS, additional LUNs are not mapped to an iSCSI target that is being used by a VJBOD disk.

VJBOD limitations

- You can create a maximum of 8 VJBOD disks.
- You can only expand an existing storage pool using VJBOD disks if the pool consists of VJBOD disks from the same storage pool on the same remote NAS.
- It is not possible to create a system volume using VJBOD disks.
- VJBOD disks only support the RAID type Single.

VJBOD automatic reconnection

If a remote NAS gets disconnected, QTS automatically tries to reconnect to the NAS and recover the VJBOD disk every 30 seconds.

Important

- To allow automatic reconnection, all NAS devices should be configured with static IP addresses.
- The following things may prevent VJBOD connection or reconnection:
  - Use of dynamic IP addresses
  - Host IQN binding
  - Firewalls of IP blocks
  - Incorrect CHAP credentials

VJBOD creation

Creating a VJBOD disk from a new LUN

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Click **Create**, and then select **Create Virtual JBOD**.
   The **Create Virtual JBOD Disk Wizard** opens.
3. Click **Next**.
4. Specify the IP address or hostname of the remote NAS.

   Important
   The remote NAS must have at least one storage pool containing at least 153 GB of free space.

   Tip
   Click **Detect** to view the IP addresses of all QNAP NAS devices on the local network. Click **Local Host** to use the IP of the local NAS.

5. Specify an administrator account and password of the remote NAS.

   Important
   For security reasons, QNAP does not recommend using the "admin" account.

6. Optional: Specify the system administration port of the remote NAS.

   Tip
   The default port is 8080. If HTTPS is enabled, the default port is 443.

7. Click **Test** to test the connection to the remote NAS.

   Important
   If prompted, complete 2-step verification. This is required if the remote NAS has enabled 2-step verification.

8. Click **Next**.
9. Optional: Select the local interface that will be used by VJBOD.
10. Optional: Select the remote interface that will be used by VJBOD.
11. Optional: Enable iSER.
    Enabling iSER increases data transfer speeds and reduces CPU and memory load.

a. Ensure that selected local and remote network adapters are iSER-compatible and have `iSER` listed under **Supported Protocols**.

b. Select **Use iSER when available**.

12. Click **Next**.
13. Select **Create a new iSCSI LUN on the remote NAS**.
14. Optional: Select **Host Binding**.
    When selected, only the local NAS will be able to access the VJBOD disk.

    Tip
    Enable this option if the VJBOD disk will be used to store sensitive information.

15. Click **Next**.
16. Select a storage pool.
17. Click **Next**.
18. Specify the capacity of the VJBOD disk.

    Important
    The size of the VJBOD disk cannot be changed after creation.

19. Optional: Configure advanced settings.

Setting	Description
4K bytes sector size	Changing the sector size to 4 KB increases LUN performance for specific applications and disk types.
SSD cache	The SSD cache will be used to improve VJBOD disk access performance.

20. Click **Next**.
    QTS starts creating a dedicated iSCSI target on the remote NAS for the VJBOD disk.
21. Optional: Enable CHAP authentication.
    An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.
    - Username
      - Length: 1 to 127 characters
      - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
    - Password
      - Length: 12 to 16 characters

- Valid characters: 0 to 9, a to z, A to Z, all special characters

22. Optional: Enable CRC checksums.
Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

23. Click **Next**.
24. Review the summary, and then click **Next**.
QTS creates the iSCSI target and LUN on the remote NAS, and then creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.
25. Select a follow-up action.

Action	Description
Create New Storage Pool	Creates a storage pool using the VJBOD disk
Create New Static Volume	Creates a static volume using the VJBOD disk
Do nothing	Ends the creation process. You can configure the VJBOD disk later. **Tip** To create a storage pool or static volume on a VJBOD disk later, go through the normal steps of creating a storage pool or static volume. Then on the disk selection screen, under **Enclosure Unit** select `Virtual JBOD`.

26. Click **Finish**.

Creating a VJBOD disk from an existing LUN

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
2. Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.
3. Click **Next**.

4. Specify the IP address or hostname of the remote NAS.

   Important
   The remote NAS must have at least one storage pool containing at least 153 GB of free space.

   Tip
   Click **Detect** to view the IP addresses of all QNAP NAS devices on the local network. Click **Local Host** to use the IP of the local NAS.

5. Specify an administrator account and password of the remote NAS.

   Important
   For security reasons, QNAP does not recommend using the "admin" account.

6. Optional: Specify the system administration port of the remote NAS.

   Tip
   The default port is 8080. If HTTPS is enabled, the default port is 443.

7. Click **Test** to test the connection to the remote NAS.

   Important
   If prompted, complete 2-step verification. This is required if the remote NAS has enabled 2-step verification.

8. Click **Next**.
9. Optional: Select the local interface that will be used by VJBOD.
10. Optional: Select the remote interface that will be used by VJBOD.
11. Optional: Enable iSER.
    Enabling iSER increases data transfer speeds and reduces CPU and memory load.

    a. Ensure that selected local and remote network adapters are iSER-compatible and have `iSER` listed under **Supported Protocols**.

    b. Select **Use iSER when available**.

12. Click **Next**.
13. Select **Choose an existing iSCSI LUN on the selected NAS**.
14. Click **Next**.

15. Select a LUN.

    Important
    The LUN must be thick and block-based, and must have a capacity of at least 154 GB.
    Mutual CHAP must be disabled.

16. Click **Next**.

17. Optional: Enable CHAP authentication.
    An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.

    - Username
      - Length: 1 to 127 characters
      - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
    - Password
      - Length: 12 to 16 characters
      - Valid characters: 0 to 9, a to z, A to Z, all special characters

18. Optional: Enable CRC checksums.
    Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

19. Click **Next**.

20. Review the summary, and then click **Next**.
    QTS creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.

21. Select a follow-up action.

Action	Description
Create New Storage Pool	Creates a storage pool using the VJBOD disk
Create New Static Volume	Creates a static volume using the VJBOD disk

Action	Description
Recover Existing Data	Restores a static volume or storage pool that was previously created on the VJBOD disk
Do nothing	Ends the creation process. You can configure the VJBOD disk later. **Tip** To create a storage pool or static volume on a VJBOD disk later, go through the normal steps of creating a storage pool or static volume. Then on the disk selection screen, under **Enclosure Unit** select `Virtual JBOD`.

22. Click **Finish**.

VJBOD management

VJBOD overview

To view an overview of all VJBOD disks including information on their source remote NAS devices, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**, click **VJBOD**, and then select **VJBOD Overview**.

VJBOD disk actions

Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**, select a VJBOD disk, and then click **Action**.

Action	Disk Status	Description
New Volume	Free	Creates a new static volume on the VJBOD disk
NAS Detail	Any	Displays information about VJBOD disk's remote NAS
Remote Log	Any	Displays the event log on the VJBOD disk's remote NAS
Data Recovery	Free	Restores a static volume or storage pool that was previously created on the VJBOD disk
Edit Disk	Any	Edits the disk name, and configure whether this disk uses the SSD cache
Disconnect	Free	Disconnects the VJBOD from its remote NAS
Connect	Disconnected	Reconnects a disconnected VJBOD disk

Action	Disk Status	Description
Edit Target	Discon-nected	Edits the following iSCSI target settings: port number, CHAP authentication, and CRC checksum settings
Detach	Data	Safely disconnects the VJBOD disk containing a storage pool or static volume. You can then connect the LUN to another NAS, create a new VJBOD disk, and recover the pool or volume using **Action** > **Data Recovery**.
Delete	Discon-nected	Deletes a VJBOD from the local disk. The LUN and all data will remain on the remote NAS You can also choose to delete the iSCSI target and LUN on the remote NAS.

Moving a VJBOD disk to another QNAP NAS

1. Note the details of the VJBOD disk's remote LUN.
   a. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.
   b. Click **VJBOD**, and then select **VJBOD Overview**.
   The **VJBOD Overview** window opens.
   c. Locate the VJBOD disk that you want to move, and then note the **Remote LUN Name** and the IP address under **Remote NAS**.
2. Detach the VJBOD disk's static volume or storage pool.
   a. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
   b. Select the static volume or storage pool on the VJBOD disk.
   c. Click **Manage**.
   The **Volume Management** or **Storage Pool Management** window opens.
   d. Click **Action**, and then select **Safely Detach**.
3. Remove the VJBOD disk from the NAS.
   a. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.
   b. Select the VJBOD disk.
   c. Click **Action**, and then select **Disconnect**.
   The status of the VJBOD disk changes to `Disconnected`.
   d. Click **Action**, and then select **Delete**.
   QTS removes the VJBOD disk from the local NAS.
4. Add the VJBOD disk on another QNAP NAS.
   a. On the other NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD**.

b. Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.

c. Click **Next**.

d. Specify the IP address or hostname of the remote NAS.

e. Specify an administrator account and password of the remote NAS.

> **Important**
> For security reasons, QNAP does not recommend using the "admin" account.

f. Optional: Specify the system administration port of the remote NAS.

> **Tip**
> The default port is 8080. If HTTPS is enabled, the default port is 443.

g. Click **Test** to test the connection to the remote NAS.

> **Important**
> If prompted, complete 2-step verification. This is required if the remote NAS has enabled 2-step verification.

h. Click **Next**.

i. Optional: Select the local interface that will be used by VJBOD.

j. Optional: Select the remote interface that will be used by VJBOD.

k. Optional: Select **Use iSER when available**.
Enabling iSER increases data transfer speeds and reduces CPU and memory load.

l. Click **Next**.

m. Select **Choose an existing iSCSI LUN on the selected NAS**.

n. Click **Next**.

o. Select the LUN containing the VJBOD disk.

p. Click **Next**.

q. Optional: Enable CRC checksums.
Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

r. Click **Next**.

s. Review the summary, and then click **Next**.
QTS creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** > **Disks**.

t. In the actions list, select **Recover Existing Data**.

u. Click **Finish**.

QTS scans for and restores any storage pools, volumes, and LUNs on the VJBOD disk.

VJBOD Cloud

VJBOD Cloud is a block-based storage gateway solution that enables you to create volumes and LUNs on your NAS using cloud space from cloud services such as Google Cloud and Amazon S3. VJBOD Cloud volumes and LUNs can utilize local storage space for accelerated read and write speeds, allowing both NAS users and applications to seamlessly and transparently access cloud storage space.

Installing VJBOD Cloud

Requirements:

- A QNAP NAS running QTS 4.4.1 or later
- A cloud space (bucket or container) with at least 1 GB of free space from a supported cloud service provider

1. Log on to QTS as administrator.
2. Ensure that a system volume is configured on the NAS.
   For details, see The system volume.
3. Open **App Center**, and then click .
   A search box appears.
4. Type `VJBOD Cloud`, and then press `ENTER`.
   The VJBOD Cloud application appears in the search results.
5. Click **Install**.
   The installation window appears.
6. Select the volume on which you want to install VJBOD Cloud.
7. Click **OK**.
   QTS installs VJBOD Cloud.

VJBOD Cloud volume and LUN creation

Creating a VJBOD Cloud volume

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
   The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud Volume**.
   The **Create VJBOD Cloud Volume** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
   Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.
   For details, see Connecting to a VJBOD Cloud service.
6. Optional: Select **Use system proxy settings**.
   When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel** > **Network & File Services** > **Network Access** > **Proxy**.
7. Click **Search**.
8. Select a cloud space.
   This may be a bucket, container, account name, or something else depending on the cloud service provider.

   Note
   If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.
9. Optional: Click **Performance test**.
   QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Create a new volume**.
12. Optional: Specify an alias for the volume.
    Alias requirements:
    - Length: 1–64 characters
    - Valid characters: A–Z, a–z, 0–9
    - Valid special characters: Hyphen (-), Underscore (_)
13. Specify the capacity of the volume.
    The amount of free space in the cloud storage space determines the maximum capacity.

Important

- The minimum volume capacity is 3 GB.
- Increasing the capacity may increase cloud storage costs. Check with the cloud service provider for details.

14. Optional: Configure any of the following 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, all data will become inaccessible.

Setting	Description	User Actions
Create a shared folder on the volume	QTS automatically creates the shared folder when the volume is ready. Only the user account that creates the shared folder has read/write access to the folder.	Specify a folder name.

15. Optional: 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.
16. Allocate stored space.
    Stored space is space used to store a copy of the volume's data locally on the NAS.
    a. Select a storage pool.
    b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the volume's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the volume's capacity	-

17. Click **Next**.
18. Review the summary information, and then click **Finish**.

The VJBOD Cloud volume appears in the **Cloud Storage** table at **VJBOD Cloud** > **Overview**.

Creating a VJBOD Cloud LUN

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
   The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud LUN**.
   The **Create VJBOD Cloud LUN** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
   Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.

For details, see Connecting to a VJBOD Cloud service.

6. Optional: Select **Use system proxy settings**.
   When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel** > **Network & File Services** > **Network Access** > **Proxy**.
7. Click **Search**.
8. Select a cloud space.
   This may be a bucket, container, account name, or something else depending on the cloud service provider.

   Note
   If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.

9. Optional: Click **Performance test**.
   QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Create a new cloud LUN**.
12. Specify a LUN name.
    Name requirements:
    - Length: 1–31 characters
    - Valid characters: A–Z, a–z, 0–9
    - Valid special characters: Underscore (_)
13. Specify the capacity of the LUN.
    The amount of free space in the cloud storage space determines the maximum capacity.

    Important
    - The minimum LUN capacity is 3 GB.
    - Increasing the capacity may increase cloud storage costs. Check with the cloud service provider for details.

14. Optional: Configure the sector size.
    Changing the sector size to 4 KB increases LUN performance for specific applications and disk types.

    Important
    VMware does not currently support a 4 KB sector size.

15. Allocate stored space.
    Stored space is space used to store a copy of the LUN's data locally on the NAS.

a. Select a storage pool.

b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the LUN's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the LUN's capacity	-

16. Click **Next**.
17. Optional: Deselect **Do not map it to a target for now**.
    If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.
18. Review the summary information, and then click **Finish**.

The VJBOD Cloud LUN appears in the **Cloud Storage** table at **VJBOD Cloud** > **Overview**.

Reattaching an existing VJBOD Cloud volume

Note

- QTS uses shared folders instead of volumes. For this reason, after creating a VJBOD Cloud volume QTS automatically creates a shared folder with the same name which is stored on the volume. You can then write data to the shared folder.
- When transferring a VJBOD Cloud volume from QuTS hero to QTS, ensure that all files are in subfolders. Files in the shared folder that are not in a subfolder will not be visible in QTS.

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
   The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud Volume**.
   The **Create VJBOD Cloud Volume** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
   Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.
   For details, see Connecting to a VJBOD Cloud service.
6. Optional: Select **Use system proxy settings**.
   When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel** > **Network & File Services** > **Network Access** > **Proxy**.

7. Click **Search**.
8. Select a cloud space.
   This may be a bucket, container, account name, or something else depending on the cloud service provider.

   Note
   If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.

9. Optional: Click **Performance test**.
   QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Attach an existing cloud volume**.
12. Select an existing volume.
13. Allocate stored space.
    Stored space is space used to store a copy of the volume's data locally on the NAS.
    a. Select a storage pool.
    b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the volume's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the volume's capacity	-

14. Click **Next**.
15. Optional: Forcibly disconnect the volume from its current NAS.
    If a volume is connected to another NAS, then the volume's status will be `Occupied` and **Current NAS** will display an IP address other than `Localhost`.

    Warning
    Forcibly disconnecting a volume deletes the volume's data from the other NAS, and then recreates the volume locally from its last restore point. Any changes to data made since the last restore point will be lost.

   a. Specify the admin password of the other NAS.

   b. Click **OK**.

16. Review the summary information, and then click **Finish**.

The VJBOD Cloud volume appears in the **Cloud Storage** table at **VJBOD Cloud** > **Overview**.

QTS automatically creates a shared folder on the volume. The shared folder has the same name as the volume.

Reattaching an existing VJBOD Cloud LUN

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
   The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud LUN**.
   The **Create VJBOD Cloud LUN** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
   Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.
   For details, see Connecting to a VJBOD Cloud service.
6. Optional: Select **Use system proxy settings**.
   When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel** > **Network & File Services** > **Network Access** > **Proxy**.
7. Click **Search**.
8. Select a cloud space.
   This may be a bucket, container, account name, or something else depending on the cloud service provider.

   Note
   If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.

9. Optional: Click **Performance test**.
   QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Attach an existing cloud LUN**.
12. Select an existing LUN.
13. Allocate stored space.
    Stored space is space used to store a copy of the LUN's data locally on the NAS.

a. Select a storage pool.

b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the LUN's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the LUN's capacity	-

14. Click **Next**.

15. Optional: Forcibly disconnect the LUN from its current NAS.
If a volume is connected to another NAS, then the LUN's status will be `Occupied` and **Current NAS** will display an IP address other than `Localhost`.

Warning
Forcibly disconnecting a LUN deletes the LUN's data from the other NAS, and then recreates the LUN locally from its last restore point. Any changes to data made since the last restore point will be lost.

a. Specify the admin password of the other NAS.

b. Click **OK**.

16. Optional: Deselect **Do not map it to a target for now**.
If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.

17. Review the summary information, and then click **Finish**.

The VJBOD Cloud LUN appears in the **Cloud Storage** table at **VJBOD Cloud** > **Overview**.

Connecting to a VJBOD Cloud service

Refer to this table when configuring a cloud service for a VJBOD Cloud volume or LUN.

Cloud Service	Steps
Alibaba Cloud OSS	**1.** Select **AlibabaCloudOSS**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**. **Note** If transfer acceleration is enabled on the bucket, VJBOD Cloud automatically enables transfer acceleration on the NAS and displays a confirmation message.
Amazon S3	**1.** Select **AmazonS3**. **2.** Select a cloud service: • **AWS Global** • **AWS China** • **AWS GovCloud (US)**: Select either **Standard** or **FIPS** protocol. • **S3 Compatible**: Specify the server address. **3.** Specify the access key. **4.** Specify the secret key. **5.** Optional: Select **Enable secure connection (SSL)**. **6.** Optional: Select **Validate SSL certificate**.
Microsoft Azure	**1.** Select **Azure**. **2.** Specify the storage account. **3.** Specify the access key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.

Cloud Service	Steps
Backblaze	1. Select **Backblaze**. 2. Specify the key ID. 3. Specify the application key. 4. Optional: Select **Validate SSL certificate**.
Catalyst	1. Select **Catalyst**. 2. Specify the user ID. 3. Specify the password. 4. Specify the project name. 5. Optional: Select **Validate SSL certificate**.
Cynny Space	1. Select **Cynny Space**. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select **Enable secure connection (SSL)**. 5. Optional: Select **Validate SSL certificate**.
DigitalOcean	1. Select **Digital Ocean**. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select **Enable secure connection (SSL)**. 5. Select a region.

Cloud Service	Steps
DreamObjects	**1.** Select **DreamObjects**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
Google Cloud Storage (P12 Key)	**1.** Select **GoogleCloudStorage**. **2.** Select **P12 key**. **3.** Specify the project ID. **4.** Specify the email address. **5.** Click **Browse**, and then select the P12 key file. **6.** Optional: Select **Validate SSL certificate**.
Google Cloud Storage (JSON Key)	**1.** Select **GoogleCloudStorage**. **2.** Select **JSON key**. **3.** Specify the project ID. **4.** Specify the email address. **5.** Click **Browse**, and then select the JSON key file. **6.** Optional: Select **Validate SSL certificate**.
Google Cloud Storage (OAuth)	**1.** Select **GoogleCloudStorage**. **2.** Select **OAuth**. **3.** Specify the project ID. **4.** Optional: Select **Validate SSL certificate**.

Cloud Service	Steps
HiCloud	**1.** Select **HiCloud**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
HKT Cloud Storage	**1.** Select **HKT**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
Huawei Cloud OBS	**1.** Select **HuaweiCloudOBS**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
IBM Cloud	**1.** Select **IBM Cloud**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.

Cloud Service	Steps
luckycloud S3	1. Select **luckycloud S3**. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select **Validate SSL certificate**.
Oracle Cloud	1. Select **Oracle Cloud**. 2. Specify the name space. 3. Specify the access key. 4. Specify the secret key. 5. Optional: Select **Enable secure connection (SSL)**. 6. Optional: Select **Validate SSL certificate**. 7. Select a region.
Qcloud Italy	1. Select **Qcloud IT**. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select **Enable secure connection (SSL)**. 5. Optional: Select **Validate SSL certificate**.
Rackspace	1. Select **Rackspace**. 2. Specify the user ID. 3. Specify the password. 4. Optional: Select **Validate SSL certificate**. 5. Select a region.

Cloud Service	Steps
S3 Compatible	**1.** Select **S3 Compatible**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Specify the authentication service. **5.** Select a signature version. **6.** Optional: Select **Enable secure connection (SSL)**. **7.** Optional: Select **Validate SSL certificate**. **8.** Optional: Specify a region.
Swift	**1.** Select **Swift**. **2.** Optional: Enable keystone authentication. **a.** Select **Enable Keystone Auth**. **b.** Specify a tenant ID or tenant name. **3.** Select the large object type. **4.** Specify the user ID. **5.** Specify the auth service. **6.** Specify the API key or password. **7.** Optional: Select **Validate SSL certificate**.

Cloud Service	Steps
Swift (Keystone v3)	1. Select **Swift**. 2. Select **Enable Keystone Auth**. 3. Select **V3**. 4. Specify a project name or project ID. 5. Specify the domain name. 6. Select the large object type. 7. Specify the user name. 8. Specify the auth service. 9. Specify the password. 10. Optional: Select **Validate SSL certificate**. 11. Select a region.
Wasabi	1. Select **Wasabi**. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select **Enable secure connection (SSL)**. 5. Optional: Select **Validate SSL certificate**.

VJBOD Cloud management

You can manage VJBOD Cloud volumes and LUNs by going to **VJBOD Cloud** > **Overview**. Select a volume or LUN and then click **Manage**.

Volume actions

Action	Description	Steps
Resize volume	Increase or decrease the size of the volume.	1. Click **Resize Volume**. 2. Specify the new capacity of the volume. 3. Select the unit of storage space. 4. Optional: Click **Set to Max** to set the capacity of the volume equal to all free space in the cloud space. 5. Click **Apply**.
Utilization	View statistics showing data uploaded, data downloaded, and cache space utilization for the volume.	Click **Actions**, and then select **Utilization**.
Set Threshold	QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.	1. Click **Actions**, and then select **Set Threshold**. 2. Enable **Please input the alert threshold [1-100]**. 3. Specify the alert threshold. 4. Click **Apply**.
Check file system	A file system check scans for and automatically repairs errors in the file system of the volume.	1. Click **Actions**, and then select **Check File System**. 2. Click **OK**.
Recovery	QTS periodically takes snapshots of a VJBOD Cloud volume. You can use these recovery point snapshots to restore the volume to a previous state.	For details, see Recovering a VJBOD Cloud volume or LUN.

LUN actions

Action	Description	Steps
Expand LUN	Increase the capacity of the LUN or its stored space.	1. Click **Expand LUN**. 2. Specify the new capacity of the LUN or its stored space, in GB. 3. Optional: Click **Set to Max** to set the capacity of the LUN equal to all free space in the cloud space. 4. Click **Apply**.
Utilization Info	View statistics showing data uploaded, data downloaded, and cache space utilization for the LUN.	Click **Actions**, and then select **Utilization**.
Recovery	QTS periodically takes snapshots of a VJBOD Cloud LUN. You can use these recovery point snapshots to restore the LUN to a previous state.	For details, see Recovering a VJBOD Cloud volume or LUN.

Volume/LUN connection status

Status	Description
Ready	The cloud storage space is working normally.
Syncing	A volume or LUN is currently syncing with the cloud space.
License Expiring	The VJBOD Cloud license attached to this storage space will expire within one month. You must renew it if you want to continue using volumes and LUNs in this storage space.
License Expired	The license attached to this storage space has expired. All volumes and LUNs created in this storage space are set to read-only.
Not Ready	There is a problem with the connection to this storage space.

Volume/LUN connection actions

To perform one of the following actions go to **VJBOD Cloud** > **Overview**, select a VJBOD Cloud volume or LUN, click **Manage**, and then click **Connection**.

Action	Description
Connect	Reconnects the volume or LUN to the cloud space.
Disconnect	Disconnects the volume or LUN from the cloud space. The volume or LUN becomes read-only.
Edit	Edits the volume or LUN's cloud space connection details.
Remove	Remove the volume or LUN from the NAS and delete all of its data from the cloud space. **Important** If QTS is unable to connect to the cloud service provider, then the volume or LUN will be removed from the local NAS but its data might be left in the cloud space.
Safely Detach	Removes the volume or LUN from the NAS but do not delete its data from the cloud space. The volume or LUN can be reattached to this NAS or another NAS later. **Important** • QTS moves all non-uploaded data in the write cache to the cloud space before removing the volume or LUN. This process may take a long time to complete. • If it's not possible to connect to the cloud space, the detach operation will fail. **Force Detach**: QTS removes the volume or LUN from the local NAS and leaves its data in the cloud space. If it's not possible to connect to the cloud space, QTS will still delete the volume or LUN from the local NAS. **Warning** If **Force Detach** is selected, non-uploaded data stored in the volume or LUN might be deleted.

Recovering a VJBOD Cloud volume or LUN

QTS periodically takes recovery point snapshots of each VJBOD Cloud volume and LUN to ensure that the volume or LUN can be recovered if it encounters an error. You can use these recovery points to restore the volume or LUN to a previous state.

1. Go to **VJBOD Cloud** > **Overview**.

2. Under **Cloud Storage**, select a VJBOD Cloud volume or LUN.
3. Click **Manage**.
   The volume or LUN management window opens.
4. Click **Actions**, and then select **Recovery**.
   The **VJBOD Cloud Volume/LUN Recovery** window opens.
5. Select a recovery point.

   Warning
   All changes to data made after the recovery point will be deleted.

6. Click **Recover**.

The status of the volume or LUN changes to `Recovering`, and then changes back to `ready` when the recovery process has finished.

Transfer resources

In VJBOD Cloud, transfer resources correspond to data uploads and downloads. If VJBOD Cloud has 100 total transfer resources, that means the application can create 100 threads for uploading data to and downloading data from the cloud.

The total transfer resources allocated to VJBOD Cloud is determined by your NAS hardware. You can manage transfer resources by going to **VJBOD Cloud** > **Transfer Resources**.

Transfer resource allocation

By default, transfer resources are shared between all VJBOD Cloud volumes and LUNs. When a volume or LUN needs to upload to or download data from the cloud, VJBOD Cloud removes transfer resources from the shared transfer resource pool and temporarily allocates them to the volume or LUN, then returns them to the pool after the data transfer has finished.

A single volume or LUN may use a large number of shared transfer resources, stopping other volumes and LUNs from syncing data with the cloud. To prevent this you can reserve transfer resources for a volume or LUN, guaranteeing that those resources will always be available. You can also set a limit on the maximum number of transfer resources a volume or LUN can use.

Transfer resource usage guidelines

Problem	Solution
VJBOD Cloud is taking a long time to sync data to the cloud.	Increase the total number of transfer resources allocated to VJBOD Cloud.

Problem	Solution
VJBOD Cloud is using too much NAS memory, CPU, or network bandwidth.	Decrease the total number of transfer resources allocated to VJBOD Cloud.
• A VJBOD Cloud volume or LUN is taking a long time to sync data to the cloud. • A VJBOD Cloud volume or LUN contains important data, which should always be backed up before other volumes and LUN data.	Increase the transfer resources reserved for the volume or LUN.
A VJBOD Cloud volume or LUN is using too many transfer resources or too much network bandwidth.	Limit the maximum number of transfer resources the volume or LUN can use.

Configuring total transfer resources

1. Go to **VJBOD Cloud** > **Transfer Resources**.
2. Under **Total resources**, specify the total number of transfer resources available to VJBOD Cloud. The minimum number is one. The maximum number is determined by your NAS hardware.

   Important
   Total transfer resources must be greater than the current reserved transfer resources.

3. Click **Apply**.

Configuring transfer resources for a volume or LUN

1. Go to **VJBOD Cloud** > **Transfer Resources**.
2. Under **Cloud Volume/LUN Resources**, locate a VJBOD Cloud volume or LUN.
3. Configure any of the following settings.

Setting	Description
Reserved	The number of transfer resources reserved for this volume or LUN.
Limit	The maximum number of transfer resources this volume or LUN can use. **Note** To set this value, **Limitation Rule** must be set to `Limit`.

Setting	Description
Limitation Rule	Select one of the following rules: • Limit: The maximum number of transfer resources this volume or LUN can use is restricted. It can only use the number specified under **Limit**. • No Limit: The maximum number of transfer resources this volume or LUN can use is unrestricted. It can use all of its reserved resources and all shared transfer resources.

4. Click **Apply**.

Event logs

Event logs, error messages, and warnings related to VJBOD Cloud are displayed in **VJBOD Cloud** > **Event Logs**. You can view logs by severity level, search logs using keywords, and configure notification settings.

VJBOD Cloud licenses

You can go to **VJBOD Cloud** > **Licenses** to view how many VJBOD Cloud licenses are registered to the local NAS, and how many of those licenses are currently being used. You can also purchase additional VJBOD Cloud licenses.

VJBOD Cloud licensing overview

VJBOD Cloud requires a license for each connection to a unique cloud space. A cloud space may be called a bucket, container, account name, or something else depending on the cloud service provider. For example, the following VJBOD Cloud volumes and LUNs require three licenses:

- *Amazon S3 → Bucket1 → Volume1*
- *Amazon S3 → Bucket2 → Volume2*
- *Azure → Space1 → LUN1*

Each unique cloud space can contain an unlimited number of VJBOD Cloud volumes and LUNs. For example, the following VJBOD Cloud volumes and LUNs require only one license:

- *Amazon S3 → Bucket1 → Volume1*
- *Amazon S3 → Bucket1 → Volume2*
- *Amazon S3 → Bucket1 → LUN1*

If a license expires, all VJBOD Cloud volumes and LUNs created from the cloud space attached to the license become read-only until the license is renewed.

VJBOD Cloud includes one free license.

Purchasing VJBOD Cloud licenses

1. Go to **VJBOD Cloud** > **Licenses**.
2. Click **Purchase License**.
   The **License Center** window opens.
3. Click **Software Store**.
4. Locate **VJBOD Cloud**, and then click **Buy**.
5. Follow the onscreen instructions to purchase and activate the VJBOD Cloud licenses.

8. iSCSI & Fibre Channel

> **Note**
> This utility is only accessible to administrators and users with the System Management role.

iSCSI & Fibre Channel is a QTS utility that enables you to configure iSCSI and Fibre Channel storage settings on your NAS.

Storage limits

iSCSI storage limits

iSCSI Storage Limit	Maximum
iSCSI LUNs and targets per NAS	255 (combined)
Connections per iSCSI session	8
iSCSI sessions per target	The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth.
iSCSI sessions per NAS	The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth.

Fibre Channel storage limits

Fibre Channel Storage Limit	Maximum
Fibre Channel ports + port groups	256 (combined)
WWPN aliases	256
LUN masking rules	256
Port binding rules	256
LUNs mapped to 1 Fibre Channel port	256

iSCSI & Fibre Channel global settings

You can configure global settings in **Global Settings**.

Setting	Description
iSCSI Service	• **iSCSI service port**: View the port used for connections from iSCSI initiators. The default port is 3260. • **Enable iSNS**: SNS enables the automatic discovery and management of iSCSI initiators and targets within a TCP/IP network. • **iSNS server IP**: Specify the IP address of the iSNS server.

Default iSCSI CHAP	CHAP authentication provides security without using NAS usernames or passwords. After configuring default iSCSI CHAP authentication settings, you can apply the default settings to an iSCSI target during target configuration, instead of configuring them manually for each target.
	• **Default iSCSI CHAP authentication**: One-way CHAP forces iSCSI initiators to authenticate when connecting to a target.
	• **Default iSCSI mutual CHAP authentication**: Mutual CHAP forces both the initiator and target to authenticate each other.
	Username and password requirements:
	• Username
	  • Length: 1 to 127 characters
	  • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
	• Password
	  • Length: 12 to 16 characters
	  • Valid characters: 0 to 9, a to z, A to Z
	Note
	To modify the default iSCSI CHAP authentication settings later, you must first disconnect all targets that are using the default settings.

LUNs

QNAP NAS devices allow other devices to access their storage space in the form of LUNs over iSCSI and Fibre Channel networks. The LUNs must first be created on the NAS, and then mapped to iSCSI targets or Fibre Channel port groups for access over the network.

QTS LUN types

QTS supports the following types of LUNs.

Tip
Block-based LUNs support more features and have faster read/write speeds. QNAP recommends using block-based LUNs over file-based LUNs if possible.

Feature	Block-based LUN	File-based LUN	VJBOD Cloud LUN
Parent storage space	Storage pool	Thick volume	Cloud space
VAAI Full Copy	Supported	Supported	Supported
VAAI Block Zeroing	Supported	Supported	Supported
VAAI Hardware-Assisted Locking	Supported	Supported	Supported
VAAI Thin Provisioning and Space Reclaim	Supported	Not supported	Supported
Thin provisioning	Supported	Supported	Not supported
QTS space reclamation	Supported (when using VAAI or the host is Windows Server 2012, Windows 8 or later)	Not supported	Supported (when using VAAI or the host is Windows Server 2012, Windows 8 or later)
Microsoft ODX	Supported	Not supported	Supported
LUN export	Supported	Supported	Supported
LUN snapshots	Supported	Partially supported (You can take a snapshot of the LUN's parent volume.)	Supported
Read/write speeds	High	Medium to low	High when using caching (stored space) Low when not using caching

Creating a block-based LUN

1. Go to one of the following screens.
   - **iSCSI & Fibre Channel** > **iSCSI Storage**

- **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**

2. Click **Create**, and then select **New Block-Based LUN**.
   The **Block-Based LUN Creation Wizard** opens.
3. Select the storage pool that this LUN will be created in.
4. Select a LUN allocation method.

Allocation	Description
Thick instant allocation	QTS allocates storage pool space when creating the LUN. This space is guaranteed to be available later.
Thin provisioning	QTS allocates storage pool space only when needed, such as when data is being written to the LUN. This ensures efficient use of space but there is no guarantee that space will be available.

5. Click **Next**.
6. Configure the following LUN settings.

Setting	Description
LUN name	• Length: 1 to 32 characters • Valid characters: 0-9, a-z, A-Z, underscore (_)
LUN capacity	Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method: • Thick provisioning: Equal to the amount of free space in the parent storage pool. • Thin provisioning: 250 TB **Tip** Select **Maximum** to allocate all remaining free space to the LUN.

7. Optional: Configure any of the following advanced settings.

Setting	Description
Sector size	Changing the sector size to 4 KB increases LUN performance for specific applications and disk types. **Important** VMware does not currently support a 4 KB sector size.
Alert threshold	QTS issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold.
Accelerate performance with SSD cache	The SSD cache will be used to improve LUN access performance. **Important** This setting is only available when the SSD cache is enabled.
Report volatile write cache for data safety	When enabled, QTS informs iSCSI initiators connected to this LUN that volatile write-cache is being used on the NAS. As a result, initiators might frequently tell QTS to flush cached LUN data to disk, which increases data safety but decreases LUN performance.
FUA bit support	When enabled, iSCSI initiators are able to tell QTS to flush important cached data to disk, instead of the whole read-write cache. **Important** Both the iSCSI initiator and the application using the LUN must support this feature.

8. Click **Next**.
9. Optional: Deselect **Do not map it to a target for now**.
   If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.
10. Click **Finish**.
11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.
    For details, see the following topics:
    - Mapping a LUN to an iSCSI target
    - Mapping a LUN to a Fibre Channel port group

Creating a file-based LUN

1. Go to one of the following screens.
   - **iSCSI & Fibre Channel** > **iSCSI Storage**
   - **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**
2. Click **Create**, and then select **New File-Based LUN**.
   The **File-Based LUN Creation Wizard** opens.
3. Select the thick volume that this LUN will be created on.
4. Select a LUN allocation method.

Allocation	Description
Thick instant allocation	QTS allocates storage pool space when creating the LUN. This space is guaranteed to be available later.
Thin provisioning	QTS allocates storage pool space only when needed, such as when data is being written to the LUN. This ensures efficient use of space but there is no guarantee that space will be available.

5. Click **Next**.
6. Configure the following LUN settings.

Setting	Description
LUN name	• Length: 1 to 32 characters • Valid characters: 0-9, a-z, A-Z, underscore (_)
LUN capacity	Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method: • Thick provisioning: Equal to the amount of free space in the parent storage pool. • Thin provisioning: 250 TB

7. Optional: Configure any of the following advanced settings.

Setting	Description
Sector size	Changing the sector size to 4 KB increases LUN performance for specific applications and disk types. **Important** VMware does not currently support a 4 KB sector size.
Alert threshold	QTS issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold.
Report volatile write cache for data safety	When enabled, QTS informs iSCSI initiators connected to this LUN that volatile write-cache is being used on the NAS. As a result, initiators might frequently tell QTS to flush cached LUN data to disk, which increases data safety but decreases LUN performance.
FUA bit support	When enabled, iSCSI initiators are able to tell QTS to flush important cached data to disk, instead of the whole read-write cache. **Important** Both the iSCSI initiator and the application using the LUN must support this feature.

8. Click **Next**.
9. Optional: Deselect **Do not map it to a target for now**.
   If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.
10. Click **Finish**.
11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.
    For details, see the following topics:
    - Mapping a LUN to an iSCSI target
    - Mapping a LUN to a Fibre Channel port group

LUN import and export

On the **LUN Import/Export** screen, you can back up a LUN as an image file to an SMB or NFS file server, local NAS folder, or external storage device. You can then import the LUN image file and restore the LUN on any QNAP NAS.

Creating a LUN export job

1. Go to **iSCSI & Fibre Channel** > **LUN Import/Export**.

2. Click **Create a Job**.
   The **Create LUN Export Job** windows opens.
3. Select **Export a LUN**.
4. Select a LUN.
5. Optional: Specify a job name.
   The name must consist of 1 to 55 characters from any of the following groups:
   - Letters: A to Z, a to z
   - Numbers: 0 to 9
   - Special characters: Underscore (_)
6. Click **Next**.
7. Select the destination folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	• IP address or host name • NFS folder or path
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	• IP address or host name • Username • Password • CIFS/SMB folder or path
Local Host	Local NAS shared folder or connected external storage device	• NAS shared folder or external device • Sub-folder

8. Click **Next**.
9. Optional: Specify a LUN image name.
   - The name 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: Underscore (_), hyphen (-), space ( )
   - The name cannot begin or end with a space.
10. Optional: Select **Use Compression** to compress the image file.
    When enabled, the image file will be smaller but exporting will take longer and will use more processor resources.

11. Select when the job will run.

Option	Description
Now	Run the job immediately after the job has been created. After this first run, the job will only run when manually started.
• Hourly • Daily • Weekly • Monthly	Run the job periodically according to the specified schedule.

12. Click **Next**.
13. Click **Apply**.

QTS creates the job. The job then starts running if **Now** was selected as the scheduling option.

Importing a LUN from an image file

1. Go to **iSCSI & Fibre Channel** > **LUN Import/Export**.
2. Click **Create a Job**.
   The **Create LUN Export Job** windows opens.
3. Select **Import a LUN**.
4. Optional: Specify a job name.
   The name must consist of 1 to 55 characters from any of the following groups:
   - Letters: A to Z, a to z
   - Numbers: 0 to 9
   - Special characters: Underscore (_)
5. Click **Next**.
6. Select the source folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	• IP address or host name • NFS folder or path

Option	Description	Required Information
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	• IP address or host name • Username • Password • CIFS/SMB folder or path
Local Host	Local NAS shared folder or connected external storage device	NAS shared folder or external device

7. Click **Next**.
8. Select the LUN image file.
9. Click **Next**.
10. Specify the import destination.

Option	Description	Required Information
Overwrite existing LUN	Import the image file data to an existing LUN. **Warning** All existing data on the LUN will be overwritten.	An existing LUN with the same type (block-based or file-based) as the LUN being imported
Create a new LUN	Import the image file as a new LUN.	• LUN name • LUN location. This will be a storage pool or volume.

11. Click **Next**.
12. Click **Apply**.

QTS creates the job, and then immediately runs it.

LUN import and export job actions

You can perform various actions on LUN import/export jobs by going to **iSCSI & Fibre Channel** > **LUN Import/Export**. Select a LUN import or export job and then click **Action** to select the desired action.

Action	Description
Edit	Edit the job.
Delete	Delete the job.
Start	Start the job.
Stop	Stop a running job.
View Logs	View the job's status, properties, details of its last run, and event logs.

LUN import and export job statuses

You can view LUN import and export job statuses by going to **iSCSI & Fibre Channel** > **LUN Import/Export**.

Status	Description
--	The job has not run yet.
Initializing	The job is preparing to run.
Processing	The job is running. The job's progress percentage is displayed next to the status.
Finished	The job has finished running or was canceled by a user.
Failed	The job failed. View the job's event log for details.

iSCSI

iSCSI enables computers, servers, other NAS devices, and virtual machines to access NAS storage in the form of LUNs over a TCP/IP network. Hosts can partition, format, and use the LUNs as if they were local disks.

Getting started with iSCSI

1. Create an iSCSI target on the NAS.
   For details, see Creating an iSCSI target.
2. Create a LUN on the NAS.
   A LUN is a portion of storage space, similar to a volume. LUNs are created from storage pool space (block-based) or from space in a thick volume (file-based).
   For more information, see:
   - QTS LUN types

- Creating a block-based LUN
- Creating a file-based LUN

3. Map the LUN to the iSCSI target.
   Multiple LUNs can be mapped to one target.
   For details, see iSCSI LUN actions.
4. Install an iSCSI initiator application or driver on the host.
   The host is the service, computer, or NAS device that will access the LUN.
5. Connect the iSCSI initiator to the iSCSI target on the NAS.

   Warning
   To prevent data corruption, multiple iSCSI initiators should not connect to the same LUN simultaneously.

   The LUNs mapped to the iSCSI target appear as disks on the host.
6. In the host OS, format the disks.

iSCSI performance optimization

You can optimize the performance of iSCSI by following one or more of these guidelines:

- Use thick provisioning (instant allocation). Thick provisioning gives slightly better read and write performance than thin provisioning.
- Create multiple LUNs, one for each processor thread on the NAS. For example, if the NAS has four processor threads, then you should create four or more LUNs.

  Tip
  Go to **Control Panel** > **System** > **System Status** > **System Information** > **CPU** to view the number of processor threads.
- Use separate LUNs for different applications. For example, when creating two virtual machines which intensively read and write data, you should create one LUN for each VM to distribute the load.
- You can use iSER (iSCSI Extensions for RDMA) for faster data transfers between QNAP NAS devices and VMware ESXi servers. Enabling iSER requires a compatible network card and switch. For a list of compatible network devices, see https://www.qnap.com/solution/iser.

iSCSI targets

iSCSI targets allow iSCSI initiators from other devices on the network to access mapped LUNs on the NAS. You can create multiple iSCSI targets and also map multiple LUNs to a single iSCSI target.

Creating an iSCSI target

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Click **Create**, and then select **New iSCSI Target**.
   The **iSCSI Target Creation Wizard** window opens.
3. Click **Next**.
4. Optional: Specify a different IQN.
   An IQN (iSCSI qualified name) is a unique name used to identify an iSCSI target.
   - Length: 1 to 128 characters
   - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
5. Optional: Specify a target alias.
   An alias enables you to identify the target more easily on the initiator.
   - Length: 1 to 32 characters
   - Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ( )
6. Optional: Select **Allow clustered access to this target**.
   When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously.

   Warning
   To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.
7. Optional: Enable CRC checksums.
   Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

8. Click **Next**.
9. Configure CHAP authentication settings.

   Note
   If you migrate your system to another NAS and have CHAP authentication enabled for the target, you must configure all CHAP passwords again on the new NAS. You can reuse old passwords or create new passwords.

a. Select a CHAP authentication option.

Option	Description
No CHAP	Do not use CHAP authentication for this target.
Default CHAP	Use the default CHAP authentication settings in **Global Settings** > **Default iSCSI CHAP** for this target. For details, see iSCSI & Fibre Channel global settings.
Customized CHAP	Configure unique CHAP authentication settings for this target.

b. Optional: Configure customized CHAP settings.

- One-way CHAP forces iSCSI initiators to authenticate when connecting to a target.

  Note
  This is the default CHAP setting.

- Mutual CHAP forces both the initiator and target to authenticate each other.

  Note
  Select **Mutual CHAP** to enable this feature. You can specify different usernames and passwords for one-way CHAP and mutual CHAP.

The username and password requirements are the same for one-way and mutual CHAP:

- Username
  - Length: 1 to 127 characters
  - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
- Password
  - Length: 12 to 16 characters
  - Valid characters: 0 to 9, a to z, A to Z

Note
If you want to modify these settings later, the target must be disconnected from all initiators.

10. Click **Next**.
11. Select the network interfaces that this target will use for data transmission.
12. Click **Next**.

13. Optional: Select **Create a LUN and map it to this target**.
    If selected, QTS opens the **Block-Based LUN Creation Wizard** immediately after finishing this wizard. The new LUN will then be automatically mapped to this target.
14. Click **Apply**.

QTS creates the iSCSI target, and then opens the **Block-Based LUN Creation Wizard** window if **Create a LUN and map it to this target** was selected.

Editing iSCSI target settings

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify iSCSI Target** window opens.
4. Modify any of the following settings.

Setting	Description
iSCSI Target IQN	An IQN (iSCSI qualified name) is a unique name used to identify an iSCSI target. • Length: 1 to 128 characters • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
Target Alias	An alias enables you to identify the target more easily on the initiator. • Length: 1 to 32 characters • Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ( )
Enable clustered access to the iSCSI target from multiple initiators	When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously. **Warning** To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.

Setting	Description
CRC/ Checksum	Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately. • Data Digest: The checksum can be used to verify the data portion of the PDU. • Header Digest: The checksum can be used to verify the header portion of the PDU.

Use CHAP authenti-cation	An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.
	• Username
	  • Length: 1 to 127 characters
	  • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
	• Password
	  • Length: 12 to 16 characters
	  • Valid characters: 0 to 9, a to z, A to Z

Mutual CHAP	Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.
	• Username
	  • Length: 1 to 127 characters
	  • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
	• Password
	  • Length: 12 to 16 characters
	  • Valid characters: 0 to 9, a to z, A to Z

5. Click **Apply**.

Binding an iSCSI target to a network interface

You can bind an iSCSI target to one or more network interfaces so that the iSCSI target can only be accessed via specific IP addresses.

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Select **Network Portal**.
5. Optional: Select one or more network interfaces to bind to the iSCSI target.
6. Optional: Deselect one or more network interfaces to remove from the iSCSI target.
7. Click **Apply**.

QTS applies the iSCSI target binding settings.

iSCSI target actions

You can perform various actions on iSCSI targets by going to **iSCSI & Fibre Channel** > **iSCSI Storage**. Select a target and then click **Action** to select the desired action.

Action	Description
Disable	Disable an active target and disconnect all connected iSCSI initiators.
Enable	Enable a disabled target.
Modify	Edit the target's settings. For details, see the following topics: • Editing iSCSI target settings • iSCSI target authorization
View Connections	View the IP addresses and IQN information of all iSCSI initiators connected to this target.
Delete	Disconnect all connected iSCSI initiators and delete the target. Any LUNs mapped to the target will be unmapped and then added to the unmapped LUN list.

iSCSI target status

You can view iSCSI target statuses by going to **iSCSI & Fibre Channel** > **iSCSI Storage**.

Status	Description
Ready	The target is accepting connections but no initiators are currently connected.

Status	Description
Connected	An initiator is connected to the target.
Offline	The target is not accepting connections.

iSCSI LUN management

Mapping a LUN to an iSCSI target

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select a LUN.

   Tip
   Double-click an iSCSI target to view all of its mapped LUNs.

3. Optional: If the LUN is already mapped to a target, disable the LUN.
   a. Click **Action**, and then select **Disable**.
   A confirmation message appears.
   b. Click **OK**.
   QTS disables the LUN.
4. Click **Action**, and then select **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
5. Select **Map to iSCSI target**.
6. Select an iSCSI target.
7. Optional: Select **Enable LUN**.
   If selected, QTS enables the LUN after mapping it to the target.
8. Click **OK**.

Changing the target of an iSCSI LUN

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select a mapped LUN.

   Tip
   Double-click an iSCSI target to view all of its mapped LUNs.

3. Click **Action**, and then select **Disable**.
   A confirmation message appears.

4. Click **OK.**
   QTS disables the LUN.
5. Click **Action**, and then select **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
6. Select **Map to iSCSI target**.
7. Select an iSCSI target.
8. Optional: Select **Enable LUN**.
   If selected, QTS enables the LUN after mapping it to the target.
9. Click **OK**.

Enabling async IO for an iSCSI LUN

Enabling async IO can improve the performance of a block-based LUN over an iSCSI connection, particularly for LUNs containing dual-actuator HDDs.

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select a mapped iSCSI LUN.

   Tip
   Double-click an iSCSI target to view all of its mapped LUNs.

3. Click **Action** and select **Modify**.
   The **Modify a LUN** window opens.
4. Under **Advanced Settings**, select **Async IO (read only)**.
5. Click **Apply**.

QTS enables async IO for the iSCSI LUN.

Note
If you want to disable async IO later, you must restart iSCSI & Fibre Channel service or restart the NAS in order for the change to take effect.

iSCSI LUN actions

You can perform various actions on iSCSI LUNs by going to **iSCSI & Fibre Channel** > **iSCSI Storage**. Expand a target to view its mapped LUNs, then select a LUN and click **Action** to select the desired action.

LUN Action	Description
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.
Enable	Enable the LUN if it is currently disabled.
Modify	Edit the LUN settings.
Delete	Delete the LUN and all data stored on it. **Important** • This action is only available if the LUN is unmapped. • To delete a VJBOD Cloud LUN, use the VJBOD Cloud app.
Utilization	View LUN utilization percentages over a specified period of time.
Edit LUN Mapping	Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: • Mapping a LUN to a Fibre Channel port group • Mapping a LUN to an iSCSI target
Show in Storage & Snapshots	Manage the LUN at **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
LUN Import/ Export	Export the LUN to another server, a local NAS folder, or an external storage device. For details, see LUN import and export.

iSCSI LUN status

You can view iSCSI LUN statuses by going to **iSCSI & Fibre Channel** > **iSCSI Storage**. Expand a target to view its mapped LUNs.

Status	Description
Ready	The LUN is ready to be mapped to an iSCSI target or Fibre Channel port group.
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.

Status	Description
[VOLUME_NAME] locked	The parent volume is locked. The LUN is inaccessible.
[POOL_NAME] locked	The parent storage pool is locked. The LUN is inaccessible.

iSCSI access control list

The iSCSI access control list (ACL) allows you to configure a LUN masking policy for each connected iSCSI initiator. A LUN masking policy determines which LUNs the initiator is able to see and access. If no policy is specified for an iSCSI initiator, then QTS applies the default policy to it.

Tip

- The default policy gives all iSCSI initiators full read/write access to all LUNs.
- You can edit the default policy so that all LUNs are either read-only or not visible to all iSCSI initiators, except for initiators with specific permissions from a policy.

Adding an iSCSI LUN masking policy

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.
3. Click **Add a Policy**.
   The **Add a Policy** window opens.
4. Specify the policy name.
   The name must consist of 1 to 32 characters from any of the following groups:
   - Letters: a-z, A-Z
   - Numbers: 0-9
   - Special characters: Hyphen (-), space ( ), underscore (_)
5. Specify the initiator IQN.
6. Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

> **Tip**
> Click the values in the columns to change the permissions.

7. Click **Apply**.

Editing an iSCSI LUN masking policy

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.
3. Select a policy.
4. Click **Edit**.
   The **Modifiy a Policy** window opens.
5. Optional: Edit the policy name.
   The name must consist of 1 to 32 characters from any of the following groups:
   - Letters: a-z, A-Z
   - Numbers: 0-9
   - Special characters: Hyphen (-), space ( ), underscore (_)
6. Optional: Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

> **Tip**
> Click the values in the columns to change the permissions.

7. Click **Apply**.

Deleting an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.
3. Select a policy.

4. Click **Delete**.
   A confirmation message appears.
5. Click **OK**.

iSCSI target authorization

Each iSCSI target can be configured either to allow connections from all iSCSI initiators, or to only allow connections from a list of authorized initiators.

Important
By default, iSCSI target authorization is disabled.

Configuring an iSCSI target's authorized initiators list

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow connections from the list only**.
6. Optional: Add one or more iSCSI initiators to the authorized iSCSI initiators list.
   a. Click **Add**.
   b. Specify the initiator IQN.
   c. Click **Confirm**.
   d. Repeat the previous steps for each additional iSCSI initiator that you want to add.
7. Optional: Delete one or more iSCSI initiators from the authorized iSCSI initiators list.
   a. Select an initiator IQN.
   b. Click **Delete**.
   c. Repeat the previous steps for each additional iSCSI initiator that you want to delete.
8. Click **Apply**.

Enabling iSCSI target authorization

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.

4. Click **Initiators**.
5. Select **Allow connections from the list only**.
6. Add one or more iSCSI initiators to the authorized iSCSI initiators list.
   a. Click **Add**.
   b. Specify the initiator IQN.
   c. Click **Confirm**.
7. Repeat the previous step for each additional iSCSI initiator that you want to add.
8. Click **Apply**.

Disabling iSCSI target authorization

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow all connections**.
6. Click **Apply**.

QNAP Snapshot Agent

QNAP Snapshot Agent enables QTS to take application-consistent snapshots of iSCSI LUNs on VMware or Microsoft servers. Application-consistent snapshots record the state of running applications, virtual machines, and data. When QTS takes a LUN snapshot, QNAP Snapshot Agent triggers the following actions:

- Windows: The server flushes data in memory, logs, and pending I/O transactions to the LUN before the snapshot is created.
- VMware: The server takes a virtual machine snapshot.

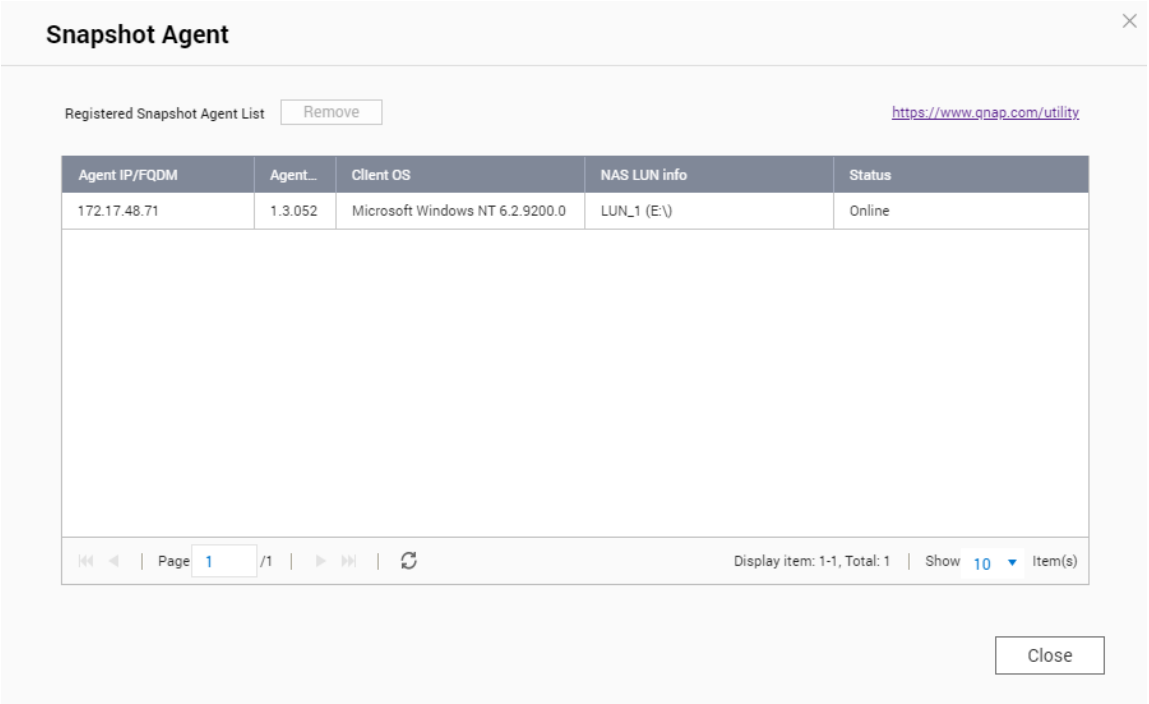
> **Tip**
> To download QNAP Snapshot Agent, go to https://www.qnap.com/utilities and then click **Enterprise**.

Snapshot Agent server list

To view a list of all iSCSI initiators that are using QNAP Snapshot Agent with this NAS, go to **iSCSI & Fibre Channel** > **iSCSI** > **iSCSI Storage**. Click **Snapshot**, and then select **Snapshot Agent**.

Tip

To unregister an iSCSI initiator, select it in the list and then click **Remove**.



Fibre Channel

Fibre Channel enables computers, servers, other NAS devices, and virtual machines to access NAS storage in the form of LUNs over a Fibre Channel network. Hosts can partition, format, and use the LUNs as if they were local disks.

Fibre Channel ports

You can view and configure Fibre Channel ports and port groups on the NAS by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports**.

Fibre Channel port groups

A Fibre Channel port group is a group of one or more Fibre Channel ports. Fibre Channel port groups help you organize and manage LUN mappings more easily. When a LUN is mapped to a Fibre Channel port group, QTS automatically maps the LUN to every Fibre Channel port in the group.

Important

- Each Fibre Channel port can be in one or more Fibre Channel port groups.
- Each LUN can only be mapped to one Fibre Chanel group.
- There is a default port group that contains all Fibre Channel ports.

Creating a Fibre Channel port group

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports**.
2. Click **Create Port Group**.
   The **Create Port Group** window opens.
3. Specify a group name.
   Name requirements:
   - Length: 1–20 characters
   - Valid characters: A–Z, a–z, 0–9
4. Select one or more Fibre Channel ports.
5. Click **Create**.

Mapping a LUN to a Fibre Channel port group

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**.
2. Select a LUN.
3. Click **Action**, and then select **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
4. Select **Map to FC port group**.
5. Select a Fibre Channel port group.

   Tip
   The default group contains all Fibre Channel ports.

6. Choose whether you want to configure LUN masking.

Option	Description
Enable LUN and do not configure LUN masking	Do not configure LUN masking. Any initiator that is able to connect to a Fibre Channel port in the port group will be able to see the LUN.
Keep LUN disabled and configure LUN masking in the next step	Configure LUN masking. You can restrict which initiators can see the LUN.

7. Click **OK**.
8. Optional: Configure LUN masking.
   a. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	1. Select one or more initiator WWPNs in the WWPN list. 2. Click **Add**.
Add WWPNs as text	1. Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` 2. Click **Add**.

   b. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
   c. Optional: Select **Enable LUN**.
   If selected, QTS enables the LUN after mapping it to the target.
   d. Click **OK**.

Configuring Fibre Channel port binding

Port binding is a Fibre Channel security method that enables you to restrict which initiator WWPNs are allowed to connect through a Fibre Channel port. It is similar to iSCSI target authorization.

Tip
By default, port binding is disabled on all Fibre Channel ports.

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports**.
2. Select a Fibre Channel port.
3. Click **Action**, and then select **Edit Port Binding**.
   The **Fibre Channel Port Binding** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	a. Select one or more initiator WWPNs in the WWPN list. b. Click **Add**.

Method	Steps
Add WWPNs as text	**a.** Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` **b.** Click **Add**.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
6. Click **OK**.

Fibre Channel port actions

You can perform various actions on Fibre Channel ports by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports**. Select a port and then click **Action** to select the desired action.

Action	Description
Edit Alias	Edit the alias for the Fibre Channel port. The alias must consist of 1 to 20 characters from any of the following groups: • Letters: A-Z, a-z • Numbers: 0-9 • Special characters: Hyphen (-), underscore (_)
View initiators	View a list of all Fibre Channel initiators currently logged into the port.
Edit port binding	Modify the port binding for the port. Port binding allows you to restrict which initiators are allowed to connect to the port. For more information, see Configuring Fibre Channel port binding.

Fibre Channel port status

You can view Fibre Channel port statuses by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports**.

Status	Description
Connected	The port has an active network connection.

Status	Description
Disconnected	The port does not have an active network connection.

Fibre Channel storage

You can manage and monitor Fibre Channel LUNs by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**.

Masking a LUN from Fibre Channel initiators

LUN masking is a security feature that enables you to make a LUN visible to some Fibre Channel initiators and invisible to other initiators.

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**.
2. Select a LUN.

   Important
   The LUN must be disabled.

3. Click **LUN Masking**.
   The **LUN Masking** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	**a.** Select one or more initiator WWPNs in the WWPN list. **b.** Click **Add**.
Add WWPNs as text	**a.** Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` **b.** Click **Add**.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
6. Select **Enable LUN**.
   If selected, QTS will enable the LUN after mapping it to the target.
7. Click **OK**.

Fibre Channel LUN actions

You can perform various actions on Fibre Channel LUNs by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**. Expand a port group to view its LUNs, then select a LUN and click **Action** to select the desired action.

LUN Action	Description
Edit LUN Mapping	Edit the LUN's mapping configuration. Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: • Mapping a LUN to a Fibre Channel port group • Mapping a LUN to an iSCSI target
Edit LUN Masking	Edit the LUN's masking configuration. LUN masking is an authorization method that makes a Logical Unit Number (LUN) visible to some initiators and invisible to other initiators. For details, see Masking a LUN from Fibre Channel initiators.
Show in Storage & Snapshots	Manage the LUN at **Storage & Snapshots** > **Storage** > **Storage/Snapshots**.
Modify	Edit the LUN settings.
Enable	Enable the LUN if it is currently disabled.
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.
Delete	Delete the LUN and all data stored on it. **Important** This action is only available if the LUN is unmapped.
LUN Import/ Export	Export the LUN to another server, a local NAS folder, or an external storage device. For details, see Creating a LUN export job.

Fibre Channel LUN status

You can view Fibre Channel LUN statuses by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**. Expand a port group to view its LUNs.

Status	Description
Ready	The LUN is ready to be mapped to an iSCSI target or Fibre Channel port group.
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.
[VOLUME_NAME] locked	The parent volume is locked. The LUN is inaccessible.
[POOL_NAME] locked	The parent storage pool is locked. The LUN is inaccessible.

Fibre Channel WWPN aliases

A WWPN (World Wide Port Name) is a unique identifier for Fibre Channel ports. A WWPN alias is a unique human-readable name for a Fibre Channel port that makes it easier to identify it.

You can view, edit, and add WWPNs and WWPN aliases by going to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.

Adding WWPNs

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
2. Click **Add**.
   The **Add WWPN** window appears.
3. Add one or more WWPNs to the list of known WWPNs using any of the following methods.

Method	Steps
Add WWPNs from logged-in Fibre Channel initiators.	Select **Add WWPNs from all logged-in FC initiators.**
Add WWPNs as text	Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX`
4. Click **Add**.

Configuring a WWPN alias

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
2. Locate a WWPN.

3. Under **Alias**, specify an alias for the WWPN.
   The alias must consist of 1 to 20 characters from any of the following groups:
   - Letters: A-Z, a-z
   - Numbers: 0-9
   - Special Characters: Underscore (_), hyphen (-)
4. Click **Save**.

Removing a WWPN alias

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
2. Locate a WWPN.
3. Clear the **Alias** field.
4. Click **Save**.

Exporting a List of WWPN aliases

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
2. Click **Export**.
   The file browser window opens.
3. In the file browser window, navigate to the folder where you want to save the file.
4. Specify a filename.
5. Click **Save**.

The list of WWPN aliases is saved to your local computer as a CSV file, in the format:

- Field 1: WWPN
- Field 2: Alias

```
11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2
```

Example CSV Output

Importing a List of WWPN aliases

You can import a list of WWPNs and aliases from a CSV file in the following format:

- Field 1: WWPN
- Field 2: Alias

```
11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2
```

Example CSV File

Important

- Identical aliases will be overwritten from the CSV file.
- Lines not formatted correctly will be ignored.

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases**.
2. Click **Import**.
   The file browser window opens.
3. Locate and open the CSV file.

9. 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.

Installing SSD Profiling Tool

1. Log on to QTS as administrator.
2. Open **App Center**, and then click  .
   A search box appears.
3. Type `SSD Profiling Tool`, and then press `ENTER`.
   The SSD Profiling Tool application appears in the search results.
4. Click **Install**.
   A confirmation window appears.
5. Click **OK**.
   QTS installs SSD Profiling Tool.

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 you to 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.

Creating an SSD over-provisioning test

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.

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	Specify the minimum and maximum amount of over-provisioning to test.
Test interval	Specify the over-provisioning increments to test.

Setting	Description
End a test phase early if consistent performance is too low	SSD Profiling Tool will end a test phase after 5 minutes of testing if the random write speeds during the phase are lower than a system-defined threshold. **Tip** Enabling this avoids wasting time testing disks when the specified amount of over-provisioning is producing no measurable benefits.

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.

Test reports

Test reports provide information to help you determine the optimal amount of over-provisioning. You can view, export, and delete test results in **SSD Profiling Tool** > **Test Reports**.

Test report information

Section	Description
Test Information	View information about the NAS, the disks being tested, and the settings used in this test.

Section	Description
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.
Temperature	View the temperature of the SSDs during each test phase.
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.

Test report actions

Icon	Description
	Open the report in a new window.
	Download a copy of the report in XLSX format.
	Delete the report.

Settings

You can configure settings in **SSD Profiling Tool** > **Settings**.

Setting	Description
Maximum number of reports	SSD Profiling Tool retains the specified number of reports. Creating additional reports deletes the oldest ones.

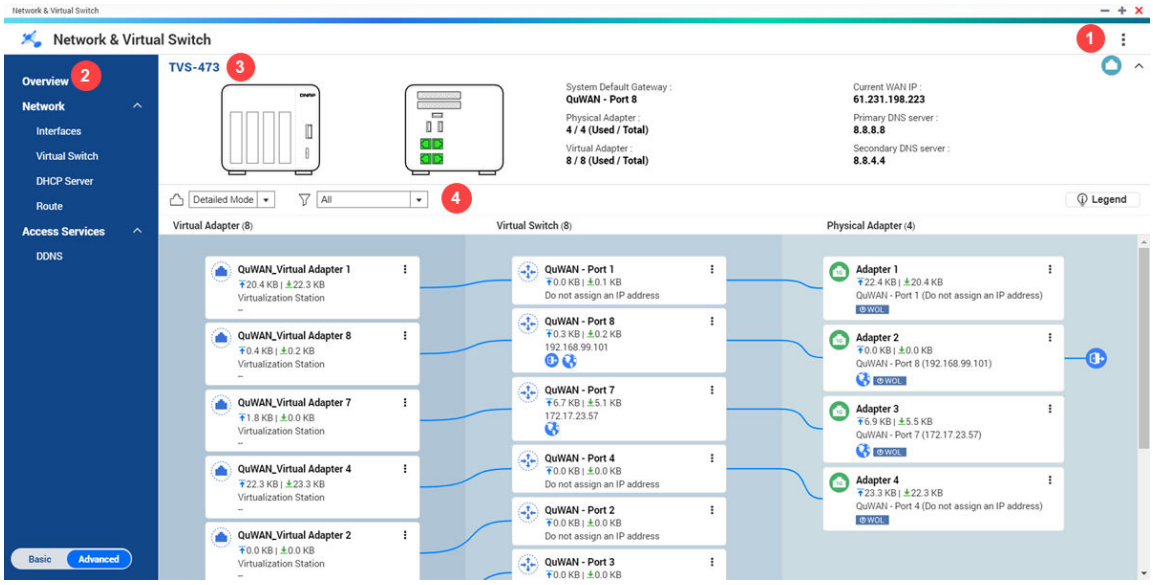
10. Network & Virtual Switch

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.

Parts of the user interface

The Network & Virtual Switch user interface has four main areas.



Label	Area	Description

1	Toolbar	The toolbar displays the following buttons:
		• **More**: Click and then select one of the following.
		  • **Quick Start**: Opens the Network & Virtual Switch guide.
		  • **Help**: Opens the Network & Virtual Switch Help panel.
		  • **About**: Displays the application version.

Label	Area	Description

2	Menu	Network & Virtual Switch features two separate usage modes in the menu pane. Switch between these modes by clicking **Basic** or **Advanced**.
		• **Basic**: This mode is well-suited for most users, and requires minimal configuration of network settings. The following functions are disabled:
		  • Static route
		  • Virtual switch
		• **Advanced**: This mode is best-suited for power-users who need more control over the configuration of network settings. The following functions are enabled:
		  • Static route
		  • Virtual switch

3	Main panel	The main panel displays the device network information. You can perform the following tasks on the main panel. •  : Click to view the MAC address of the network adapters and the virtual adapter information. • : Click to collapse the main panel.

Label	Area	Description

4	Network topology	The network topology provides a visual representation of the connected physical and virtual network adapters.
		You can perform the following tasks on the network topology panel.
		• Click the drop-down list beside to view the topology in simple or detailed mode.
		• Click the drop-down list beside to filter and view specific network topology components.
		• Click **Legend** to view the different icons and their descriptions.
		• Physical adapters: Click and select one of the following.
		  • **Locate**: Click to identify the network port on the main panel.
		  • **Setting**: Click to configure the physical adapter settings.
		• Virtual switches: Click and then click **Settings** to open the virtual switch configuration page.
		• Virtual adapters: Click and then click **Execute** to view the virtual adapter information on Virtualization Station

Basic network adapter configuration

Network & Virtual Switch allows QTS users to configure and manage the basic network adapter settings including different IP addressing methods, routing protocols, and system default gateway.

Tip
To review IP address and hardware information about an interface, go to **Interfaces**, click , and select **Information**. You can export the details to your clipboard by clicking **Copy**.

Configuring IPv4 settings

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Interfaces**.
4. Identify the adapter that you want to configure, then click > **Configure**.
   The **Configure** window opens.

5. Configure the IPv4 settings.

   a. Optional: Select **Obtain IP address settings automatically via DHCP** to allow the DHCP server on the network to automatically assign the necessary network configurations to the device.

   b. Optional: Select **Use static IP address** to manually assign the following IP information.

      - Fixed IP address
      - Subnet mask
      - Default gateway

   c. Specify a jumbo frame size.
   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 device models support Jumbo Frames.
      - Using jumbo frames requires a network speed of 1000 Mbps or faster.

   d. Select the network speed (transfer rate) allowed by the 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.

6. Click **Apply**.

Network & Virtual Switch updates the IPv4 settings.

Configuring IPv6 settings

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Interfaces**.
4. Identify the adapter that you want to configure and then click  > **Configure**.
   The **Configure** window opens.
5. Go to the **IPv6** tab.
6. Select an IPv6 setting.
   - **Disable**: Disables the IPv6 address to the network interface.
   - **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 (Obtain the prefix length information from your network administrator)
     - Default gateway (Specify a default gateway prefix between FE80 and FEB)
7. Click **Apply**.

Network & Virtual Switch updates the IPv6 settings.

Configuring the 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. You must configure a network interface first prior to assigning the default gateway.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Interfaces**.

4. Click **System Default Gateway**.
   The **System Default Gateway** window opens.
5. Select a default gateway method.
   - **Auto-select system default gateway**

Setting	User Action
Auto-select system default gateway	QTS utilizes a dynamic algorithm to analyze network interfaces and automatically designate the most suitable option as the primary route for external communication.
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.
Enable NCSI service	The Network Connectivity Status Indicator (NCSI) service verifies internet connectivity and displays the current state of the internet connection. Select one of the following NCSI service. • **QNAP NCSI Server**: The public NCSI server hosted by QNAP functions as the default target for testing purposes. • **Default Gateway**: The configured gateway IP address on the device can be specified as the target for network analysis. • **Custom Target**: Users can define a customized target by providing a specific domain name or IP address for focused network connectivity evaluation. Enter a valid domain name or IP address as the custom target

6. Click **Apply**.

Network & Virtual Switch updates the system default gateway settings.

Configuring static route settings

You can create and manage IPv4 and IPv6 static routes in the **Route** section of Network & Virtual Switch. 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.

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Route**.
4. Select a method for adding the IP static route.
   - IPv4 static route
   - IPv6 static route
5. Optional: Configure the IPv4 static route settings.
   a. Beside Main Routing Table, select **IPv4** from the drop-down menu.
   b. Click **Add**.
      The **Static Route (IPv4)** window opens.
   c. Configure the IP address settings.
      - **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.
   d. Click **Apply**.

   Network & Virtual Switch adds the IPv4 static route.
6. Optional: Configure the IPv6 static route settings.
   a. Beside Main Routing Table, select **IPv6** from the drop-down menu.
   b. Click **Add**.
      The **Static Route (IPv6)** window opens.
   c. Configure the IP address settings.
      - **Destination**: Specify a static IPv6 address where connections are routed to.
      - **Prefix Length**: Select the destination prefix length for the IPv6 static route.
      - **Next Hop**: Specify the next hop IP address in IPv6 format.

        Tip
        IPv6 next hop format: 2001:db8::1

- **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.

d. Click **Apply**.

Network & Virtual Switch adds the IPv6 static route.

Configuring IEEE 802.1X authentication

IEEE 802.1X authentication mitigates the risk of unauthorized devices gaining access to the network. When enabled on a network adapter, devices and users connected to the interface are authenticated based on the specified authentication method.

- TLS CA certificate: A digital certificate that is used to sign other TLS certificates.
- TLS user certificate: A digital certificate that is used to authenticate a user to a TLS server.
- TLS private key: A cryptographic key that is used to decrypt data that has been encrypted with a TLS public key.

Note

- Allowed file extensions for TLS certificates include .der, .pem, .crt, and .cer files.
- Allowed file extensions for private keys include .der, .pem, .p12, and .key files.
- Providing a CA certificate is optional.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Interfaces**.
4. Identify a network interface.
5. Click ⋮.
   The **Configure** window appears.
6. Go to **Security**.
7. Select **Enable IEEE 802.1X authentication**.
   A confirmation message is displayed indicating that the device password and certificate files are saved to a local storage location on the system.
8. Click **Agree**.

9. Select an authentication method.

   - **MD5**: MD5 is a cryptographic hash function that produces a unique 128-bit value from any input of any length.

     Important
     MD5 is a legacy cryptographic hash function that is vulnerable to collision attacks.

     1. Specify the account username.
     2. Specify the account password.

   - **TLS**: TLS (Transport Layer Security) uses mutual authentication, which means that both the client and the server authenticate each other.

     1. Specify the digital identity asset, such as a domain name, hostname, IP address, or URL.
     2. Next to **User certificate**, click **Import File**.
        A file explorer window appears.
     3. Select the user certificate.
     4. Click **Open**.
     5. Next to **CA certificate**, click **Import File**.
        A file explorer window appears.
     6. Click **Open**.
     7. Next to **Private key**, click **Import file**.
        A file explorer window appears.
     8. Click **Open**.
     9. Specify a password to protect the private key.

   - **Tunneled TLS**: A variation of TLS that uses a TLS tunnel to protect the authentication process from eavesdropping and tampering. This method does not use mutual authentication.

     1. Specify an anonymous identifier for the TLS tunnel to hide the device and user information.
     2. Next to **CA certificate**, click **Import File**.
        A file explorer window appears.
     3. Click **Open**.
     4. Select an inner authentication (EAP authentication inside tunneled EAP) method.
        - PAP (Password Authentication Protocol)
        - MSCHAP (Microsoft Challenge Handshake Authentication Protocol)
        - MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2)

- CHAP (Challenge Handshake Authentication Protocol)
- MD5 (Message-digest algorithm)
- GTC (Generic Token Card)

5. Specify the username and password.

- **Protected EAP**: Protected EAP (Extensible Authentication Protocol) enhances security by utilizing server certificates, client authentication, and TLS tunnels to encrypt and encapsulate EAP.

1. Specify an anonymous identity to authenticate the TLS tunnel.
2. Next to **CA certificate**, click **Import File**.
   A file explorer window appears.
3. Click **Open**.
4. Select the PEAP version.
5. Select an inner authentication (EAP authentication inside tunneled EAP) method.
   - PAP (Password Authentication Protocol)
   - MSCHAP (Microsoft Challenge Handshake Authentication Protocol)
   - MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2)
   - CHAP (Challenge Handshake Authentication Protocol)
   - MD5 (Message-digest algorithm)
   - GTC (Generic Token Card)
6. Specify the username and password.

10. Click **Apply**.

Network & Virtual Switch configures IEEE 802.1X authentication to the interface.

IP addressing services configuration

QNAP provides IP addressing services for network adaptability and scalability. You can deploy dynamic address allocation and resolution techniques such as DNS, DDNS, DHCP server, and RADVR settings to meet evolving network requirements.

Configuring DNS server settings

A Domain Name System (DNS) server translates a domain name into an IP address. You can either automatically obtain a public DNS server IP address or manually assign an IP address for the DNS server.

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:
   - **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**.

Network & Virtual Switch updates the DNS server settings.

Configuring DHCP server settings

The Dynamic Host Configuration Protocol (DHCP) allows devices in a TCP/UDP network to be automatically configured for the network as the device is booted. The DHCP service uses a client-server mechanism, wherein a DHCP server stores and manages network configuration information for clients and offers necessary data when a client requests the information. The information includes the IP address and subnet mask, the IP address of the default gateway, the DNS server IP address, and the IP lease information.

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.

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.
      1. Specify a fixed IP address.

         Tip
         Examine your network setup for guidance on how to best configure these settings.

      2. Specify the subnet mask used to subdivide your IP address.
      3. Specify the IP address of the default gateway for the adapter.
      4. Specify a jumbo frame size.

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.

5. Specify the speed at which the adapter will operate.

   Tip
   Auto-negotiation will automatically detect and set the transfer rate.

6. Assign an IP address for the primary DNS server.
7. 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.
   a. Specify the starting IP address in a range allocated to DHCP clients.
   b. Specify the ending IP addresses in a range allocated to DHCP clients.
   c. Specify the subnet mask used to subdivide your IP address.
   d. 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.
   e. Specify the IP address of the default gateway for the DHCP server.
   f. Specify a DNS server for the DHCP server.
   g. Optional: Specify a secondary DNS server for the DHCP server.

      Important
      QNAP recommends specifying at least one DNS server to allow URL lookups.

   h. 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.

i. Specify the DNS suffix.

> **Tip**
> The DNS suffix is used for resolving unqualified or incomplete host names.

j. Specify the public IP address for the TFTP server.

> **Tip**
> QTS supports both PXE and remote booting of devices.

k. Specify location and file name of the TFTP server boot file.

> **Tip**
> QTS supports both PXE and remote booting of devices.

10. Click **Apply**.

Network & Virtual Switch adds the DHCP server.

Adding DHCP clients to a DHCP server

A DHCP client is a network device using DHCP service to obtain network configuration parameters such as an IP address from a DHCP server. When a DHCP client sends a broadcast message to locate a DHCP server, the DHCP server provides configuration parameters (IP address, MAC address, domain name, and a lease for the IP address) to the client.

The following table describes the two types of DHCP clients employed in Network & Virtual Switch.

DHCP Client	Description
Physical Adapter DHCP Client	Enabling a DHCP IPv4 address allows the device to automatically acquire an IPv4 address for a specific physical adapter from a DHCP server. The physical adapter is assigned an IP address by the DHCP server for a predefined lease time. **Note** For details on obtaining a DHCP provided IP address, see Configuring IPv4 settings.

DHCP Client	Description
Virtual Switch DHCP Client	Virtual switches allow virtual machines to obtain IP-related configurations automatically from an external DHCP server. The virtual switch obtains the IP address from the DHCP server through the connected physical adapter on the device. **Note** 1. A virtual switch configured with an automatic DHCP IP address cannot utilize the NAT and DHCP server functions. 2. Virtual switches cannot automatically acquire the IP address of the physical adapter unless the virtual switch has been configured to connect to a physical adapter in **Network** > **Virtual Switch**.

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **DHCP Server**.
3. Identify a DHCP server.
4. Under Actions, click  .
   The **DHCP Client Table** window appears.
5. Click **Add Reserved IP**.
   The **Add Reserved IP** window appears.
6. Configure the DHCP client information.
   a. Specify a device name for the DHCP client.
   b. Specify the IP address of the DHCP client.
   c. Specify the MAC address of the DHCP client.
7. Click **Apply**.

Network & Virtual Switch adds the DHCP client.

Configuring RADVD server settings

This **RADVD** 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.

1. Log on to QTS as administrator.

2. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **DHCP Server**.
4. Go to the **RADVD** tab.
5. Click **Add**.
   The **RADVD - Outgoing Interface** window opens.
6. Select the outgoing interface.
7. Click **Next**.
8. 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 the static IP address settings.
      1. Specify a fixed IP address.

         Tip
         Examine your network setup for guidance on how to best configure these settings.

      2. Specify the subnet mask used to subdivide your IP address.
      3. Specify the prefix length for the adapter.

         Tip
         Obtain the prefix and the prefix length information from your ISP.

      4. Specify the IP address of the default gateway for the adapter.
      5. Specify a jumbo frame size.

         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.

      6. Specify the speed at which the adapter will operate.

> **Tip**
> **Auto-negotiation** will automatically detect and set the transfer rate.

7. Assign an IP address for the primary DNS server.
8. 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. Select a second adapter for the RADVD service interface.
10. Click **Next**.
11. 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 the static IP address settings.
c. Click **Apply**.

12. Configure the RADVD server settings.

a. Specify the routing prefix for the adapter.

> **Tip**
> Examine your network setup for guidance on how to best configure these settings.

b. Specify the prefix length for the adapter.
c. 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.
d. Specify the DNS server address.
e. Optional: Specify a secondary DNS server.

> **Important**
> QNAP recommends specifying at least one DNS server to allow URL lookups.

13. Click **Apply**.

Network & Virtual Switch adds the RADVD server.

Configuring DDNS service settings

The **DDNS** 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.

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Access Services** > **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**.

Network & Virtual Switch adds the DDNS server service.

LAN switching configuration

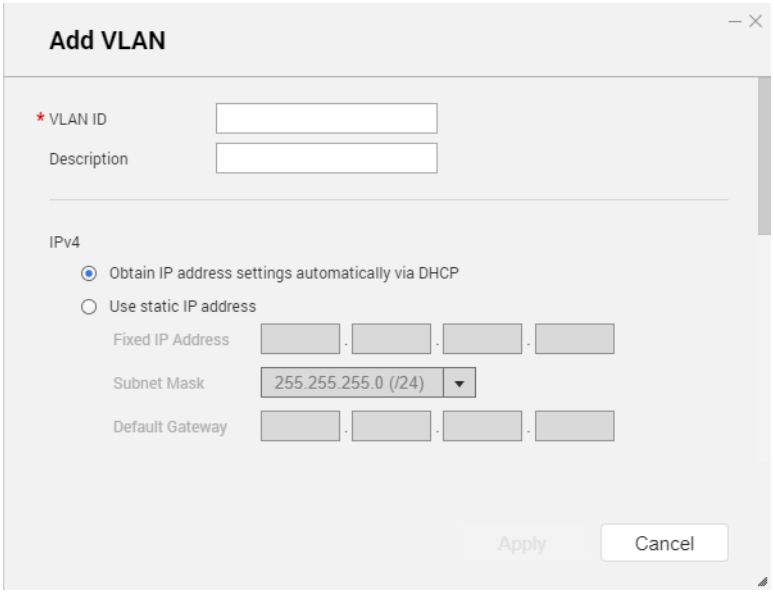
LAN switching enables users to resolve bandwidth issues by increasing the efficiency of LANs using VLAN and port trunking technologies.

Configuring VLAN settings

A virtual LAN (VLAN) groups multiple network devices together and limits the broadcast domain. Members of a VLAN are isolated and network traffic is only sent between the group members. You can use VLANs to increase security and flexibility while also decreasing network latency and load.

Important
When using both port trunking and a VLAN, port trunking must be configured first.

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 ⋮.
4. Select **Add VLAN**.
   The **Add VLAN** window opens.



5. Specify a VLAN ID.

   Important
   The VLAN ID must be between 1 and 4094.

6. Specify a description for the VLAN.
7. Select one of the following options.

Option	Steps
Automatically obtain the IP address using DHCP	Select **Obtain IP address settings automatically via DHCP**.

Option	Steps
Use a static IP address	**a.** Select **Use static IP address** **b.** Specify a fixed IP address. **c.** Select a subnet mask. **d.** Specify the default gateway.

8. Click **Apply**.

Network & Virtual Switch adds the VLAN.

Configuring port trunking settings

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.

Important
Before configuring port trunking settings, 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 secondary 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.
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.

10. Click **Apply**.

Network & Virtual Switch applies the pork trunking settings.

Virtual switch configuration

The **Virtual Switch** 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 a MAC address for the virtual switch.

   Note
   Network & Virtual Switch automatically uses the MAC address of the selected physical network adapter.
   If you do not select a physical network adapter from the list, Network & Virtual Switch assigns a random MAC address to the virtual switch.

9. Click **Next**.
10. 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.

11. Click **Next**.

12. 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.

13. Configure the DHCP server settings.

    a. Specify the starting IP address in a range allocated to DHCP clients.

    b. Specify the ending IP addresses in a range allocated to DHCP clients.

    c. Specify the subnet mask used to subdivide your IP address.

    d. 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.

    e. Specify the IP address of the default gateway for the DHCP server.

    f. Specify a DNS server for the DHCP server.

    g. Optional: Specify a secondary DNS server for the DHCP server.

    Important

    QNAP recommends specifying at least one DNS server to allow URL lookups.

h. 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.

i. Specify the DNS suffix.

> **Tip**
> The DNS suffix is used for resolving unqualified or incomplete host names.

j. Specify the public IP address for the TFTP server.

> **Tip**
> QTS supports both PXE and remote booting of devices.

k. Specify location and file name of the TFTP server boot file.

> **Tip**
> QTS supports both PXE and remote booting of devices.

14. Click **Next**.
15. Configure the virtual switch IPv6 address.
    - **Disable**: Disables the IPv6 address to the network interface.
    - **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 (Obtain the prefix length information from your network administrator)

- Default gateway (Specify a default gateway prefix between FE80 and FEB)

16. Click **Next**.
17. 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.

18. Click **Next**.
19. Confirm the virtual switch settings.
20. Click **Apply**.

Network & Virtual Switch creates a virtual switch in advanced mode.

Creating a virtual switch in software-defined switch mode

Important
To avoid bridge loops, 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**.

Network policies configuration

Network policies allow QTS users to manage data traffic by implementing data reliability policies on the network adapters of the device.

Configuring Forward Error Correction (FEC) settings

Forward Error Correction (FEC) is a digital signal processing technique to recover lost packets on a link by sending extra parity packets. Enabling FEC enhances data reliability by introduces redundant data or error correcting data before the system stores or transmits data.

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. Click **FEC Settings**.
5. Click **Enable forward error correction (FEC)**.
6. Select an FEC mode.

Setting	Description
Auto-negotiation	The device automatically selects the best FEC mode.
BASE-R FEC	BASE-R FEC (also known as Fire Code FEC or IEEE 802.3 Clause 74) offers simple, low latency (less than 100 nanoseconds) protection against bursty errors. This mode offers a weaker error correction but with lower latency.
RS-FEC	RS-FEC (also known as Reed Solomon FEC or IEEE 802.3 Clause 91) offers better error protection but adds latency (approximately 250 nanoseconds).

Important
The same FEC mode should be selected on both ends of the network link.

7. Click **Apply**.

Network & Virtual Switch applies the FEC settings.

Wireless network configuration

The Network & Virtual Switch Wi-Fi service provides all the functions of a wired network, while also providing location flexibility to QTS users within the wireless signal range. The **Wi-Fi** screen controls the configuration and management of Wi-Fi connections accessible from the device.

Important

- A USB or PCIe Wi-Fi device must be installed to access wireless 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.

Adding a wireless network

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
3. Go to **Network** > **Interfaces**.
4. Go to the **Wi-Fi** tab.
5. Click **Add Wi-Fi**.
   The **Connect to a Wi-Fi network** window opens.
6. Configure connection settings.
   a. Enter a name of the wireless network.
   b. Select the encryption used by the wireless network.
      - **No Authentication (Open)**:Any wireless device can connect to the network. This is the default setting.
      - **WEP**: Use Wired Equivalent Privacy (WEP) if the wireless device does not support WPA or WPA2.
      - **WPA- Personal**: Use Wi-Fi Protected Access (WPA)- Personal as an intermediate security measure if the wireless device does not support WPA2.
      - **WPA2-Personal**: Uses Advanced Security Encryption (AES) for data encryption. This is the suggested security mechanism if the wireless device supports WPA2.

- **WPA- & WPA2- Enterprise**: Use this security mechanism if the wireless device supports transition from WPA-Enterprise to WPA2-Enterprise. The network automatically chooses the encryption method used by the wireless device.
- **No Authentication (Open)**:Any wireless device can connect to the network. This is the default setting.
- **WEP**: Use Wired Equivalent Privacy (WEP) if the wireless device does not support WPA or WPA2.
- **WPA- Personal**: Use Wi-Fi Protected Access (WPA)- Personal as an intermediate security measure if the wireless device does not support WPA2.
- **WPA2-Personal**: Uses Advanced Security Encryption (AES) for data encryption. This is the suggested security mechanism if the wireless device supports WPA2.
- **WPA- & WPA2- Enterprise**: Use this security mechanism if the wireless device supports transition from WPA-Enterprise to WPA2-Enterprise. The network automatically chooses the encryption method used by the wireless device.

c. Enter the password provided by the network administrator.

> **Tip**
>
> Click  to make the password visible.

d. Optional: Select **Automatically connect when the Wi-Fi network is in range.**.

e. Select **Connect even if hidden** to connect to this network even if the SSID is hidden.

7. Optional: Configure WPA- & WPA2 Enterprise settings.

Setting	User Action
Authenti-cation	Select a method based on the authentication supported by your device. Authentication is specific to WPA- and WPA2- Enterprise encryption. • **Protected EAP (PEAP)**: Protected Extensible Authentication Protocol (PEAP) provides a more secure authentication to 802.11 WLANs. • **EAP-TTLS**: EAP Tunneled Transport Layer Security (EAP-TTLS) supports legacy authentication mechanisms.
Certificate Authority (CA) File	A data file that contains identification credentials to help authenticate the WPA-WPA2 public key ownership. **Note** Select **CA file is not required** if you do not have access to a digital certificate.

Setting	User Action
Inner Authentication	Select an inner authentication method based on PEAP or EAP-TTLS authentication. MS-CHAPv2 is the default inner authentication method for PEAP. The following inner authentication methods are available if the authentication method is set to EAP-TTLS: PAP, CHAP, MS-CHAP, MS-CHAPv2
Username	Enter the username provided by the network administrator.
Password	Enter the password provided by the network administrator. **Tip** Click  to make the password visible.

8. Click **Connect**.

Network & Virtual Switch adds the wireless network.

Enabling Wi-Fi

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces**.
3. Go to the **Wi-Fi** tab.
4. Click  .

Network & Virtual Switch enables the Wi-Fi function.

Connecting to a wireless network

1. Go to **Control Panel** > **Network & File Services** > **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	User Action
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**

The device connects to the wireless network.

Connecting to a captive-portal-enabled wireless network Using Browser Station

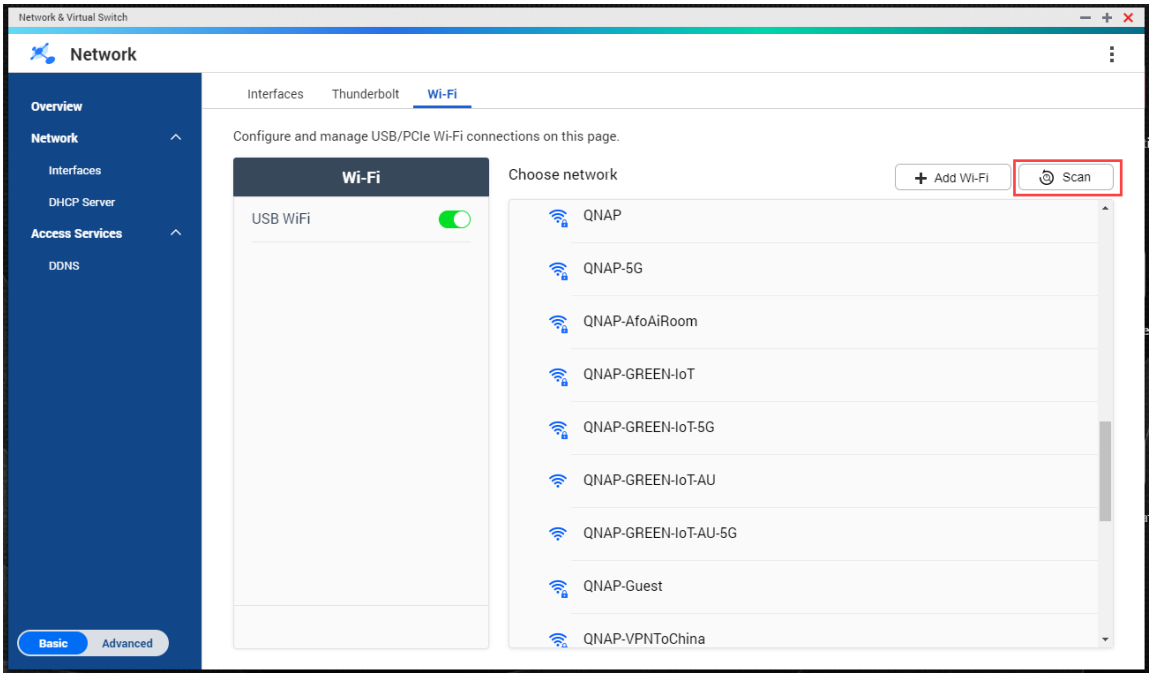
A captive portal allows organizations to easily share their network environment with customers, employees, and other guests.

QTS supports the captive portal function that connects to the internet through an access point in the wireless network.

Note

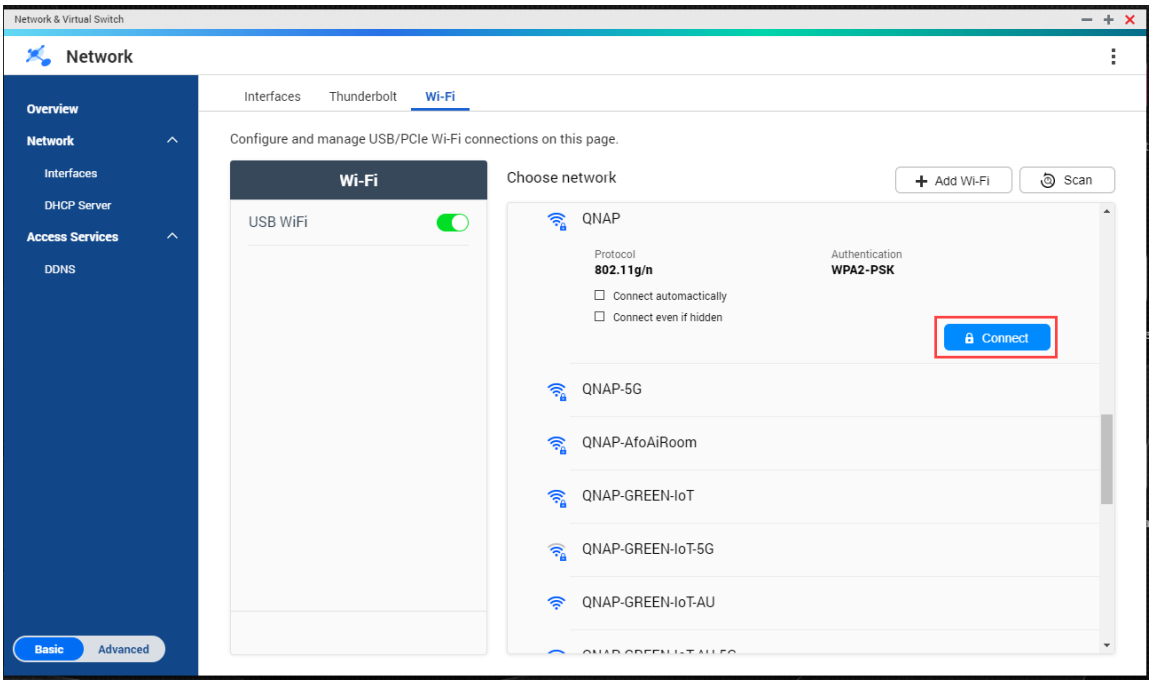
Download and install Browser Station from App Center to access the captive portal functions.
Alternatively, QNAP recommends installing Qfinder Pro (6.9.2 or later) to utilize the captive portal function on a wireless network.
For details, see Connecting to a captive-portal-enabled wireless network Using Qfinder Pro.

1. Go to **Control Panel** > **Network & File Services** > **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 wireless networks with a captive portal.

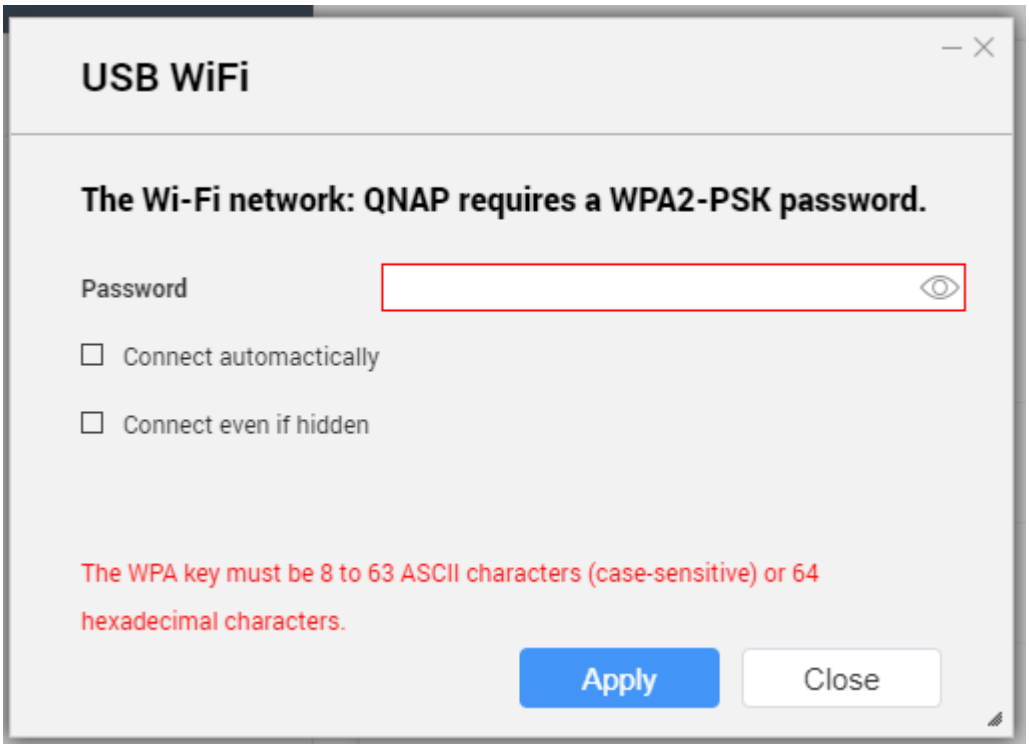


5. Select the captive-portal-enabled wireless network from the list.
   The settings panel expands.

6. Click **Connect**.

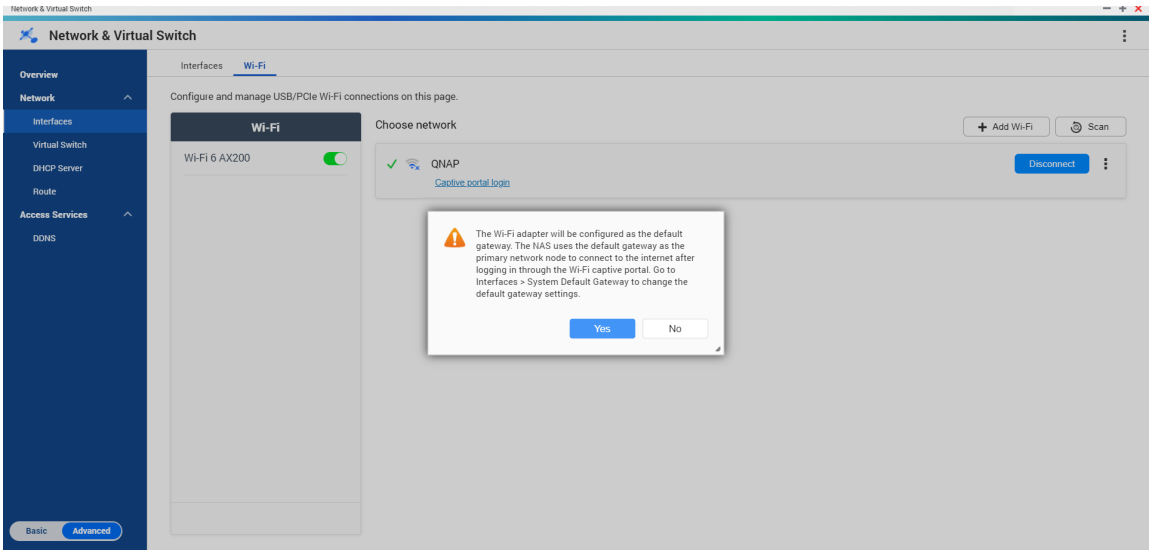


7. Optional: Configure connection settings.

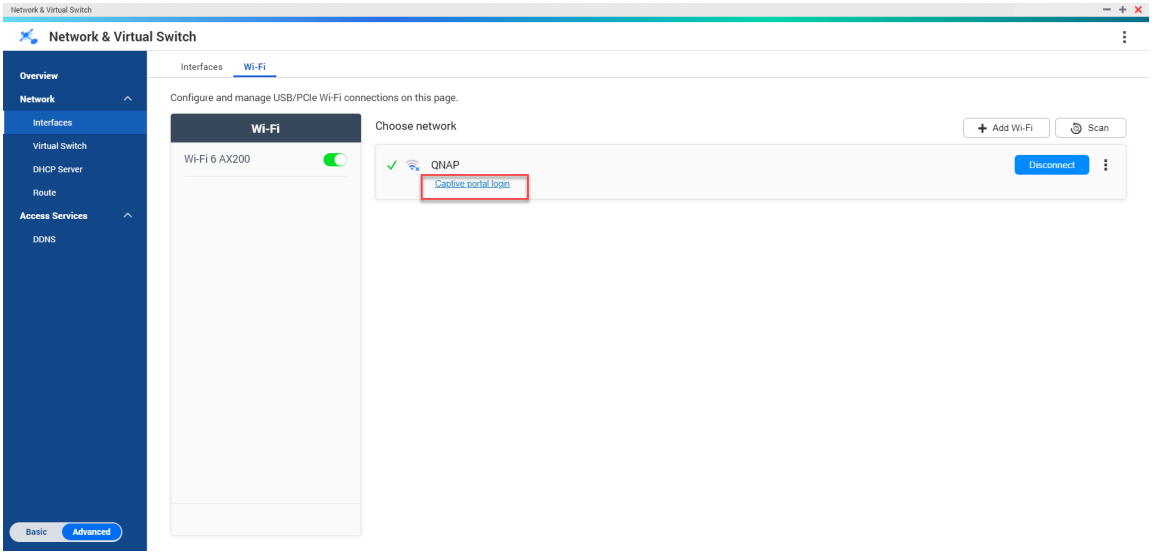


For configuration details and wireless icon descriptions, see Connecting to a wireless network.

8. Click **Apply**.
A popup window opens specifying the change in the default network gateway.



9. Click **Yes**.
10. Optional: Go to **Interfaces** > **System Default Gateway** to change the default network gateway settings.
11. Click **Captive portal login**.



Browser Station automatically redirects you to the captive portal landing page.

12. Enter the username and password to connect to the wireless network.

Connecting to a captive-portal-enabled wireless network Using Qfinder Pro

Note

QNAP recommends installing Qfinder Pro (Windows 6.9.2 or later and MacOS/Linux 7.3.2 or later) to utilize the captive portal function on a wireless network.

Important
Connect the NAS directly to the PC using an Ethernet cable in order to connect to a wireless network enabled with captive portal.

1. Open Qfinder Pro.
2. Locate the NAS in the list and click the unconfigured Wi-Fi icon located under the Status table header.
3. Optional: Alternatively, select the NAS and go to **Settings** > **Wi-Fi Settings**.
   The **Login** page opens.
4. Enter the username and password.
5. Click **OK**.
   The **Wi-Fi Connection Settings** page opens.
6. Select the wireless network from the list.
   The settings panel expands.
7. Click **Connect**.
8. Configure connection settings.
9. Click **Apply**.
   A confirmation window opens.
10. Click **Yes**.
    The default browser automatically opens and redirects you to the captive portal landing page.

    Note
    Network & Virtual Switch automatically enables NAT and DHCP on the Wi-Fi adapter in the background.

11. Enter the username and password to connect to the wireless network.

    Qfinder Pro displays the wireless connection icon in the Qfinder Pro NAS status panel.

Understanding the wireless 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.

Message	Description
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.

Accessing the wireless access point (AP) settings

The Network & Virtual Switch utility enables users to configure and manage wireless access points through the WirelessAP Station utility.

> **Note**
> The WirelessAP Station is not a built-in application on QTS 5.0.0. To install the application, go to **App Center** > **All Apps**, and then install the WirelessAP Station application.

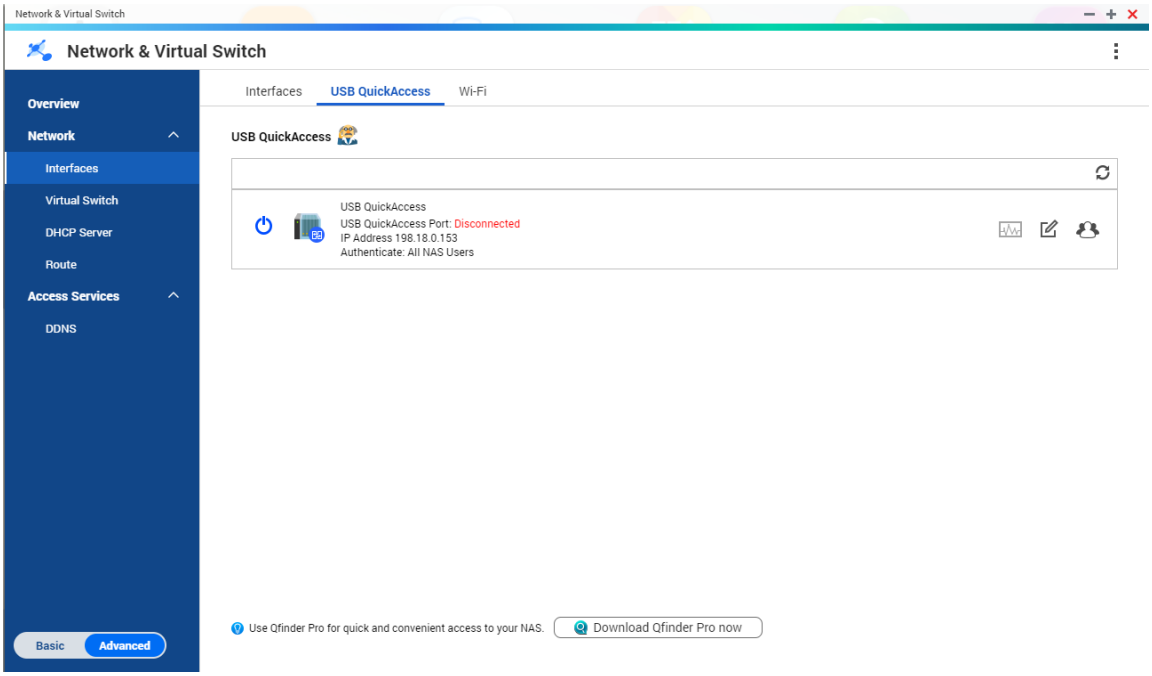
1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces**.
3. Click the **WirelessAP Station** tab.

QTS opens the WirelessAP Station application.

For details on configuring the access point settings, click ⓘ on the application taskbar.

USB QuickAccess configuration

The **USB QuickAccess** 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).



Important

- 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 & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces**.
3. Go to the **USB QuickAccess** tab.
4. Click  .

Network & Virtual Switch enables USB QuickAccess.

Configuring the USB QuickAccess IP address

1. Go to **Control Panel** > **Network & File Services** > **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 fixed IP Address.
6. Click **Apply**.

Network & Virtual Switch applies the IP address settings.

Configuring USB QuickAccess authentication

1. Go to **Control Panel** > **Network & File Services** > **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**.

Network & Virtual Switch applies the USB QuickAccess authentication settings.

Thunderbolt interface configuration

The **Thunderbolt** 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 port 2 may have connectivity problems when connecting to Windows. Thunderbolt port 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.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
sudosysctlnet.inet.tcp.path_mtu_discovery=0 && sudosysctlnet.inet.tcp.tso=0	This command will only temporarily enable T2E. Restarting the Mac will delete the connection.

Command	Notes
sudo bash –c 'printf "#QNAP\nnet.inet.tcp.path_mtu_discovery=0\nnet.inet.tcp.tso=0\n#QNAP\n" >> /etc/sysctl.conf'	This command will permanently apply these settings.

Updating the firmware of a network expansion card

If a network expansion or interface card is attached to your QNAP device, you can update the firmware of the attached card through the QTS interface.

Note

QNAP recommends keeping the expansion card firmware up-to-date. By default, QTS checks daily for firmware updates for the expansion card.

Important

- To avoid corrupting the expansion card, ensure that you do not power off or restart the device during the firmware update process.
- You must restart the device after the update process completes to apply the changes.
- Do not access the device using the network expansion card that requires an update.

1. Go to **Network & Virtual Switch** > **Interfaces**.
2. Beside an adapter, click  .
   The **Network Expansion Card Firmware Update** window appears.
3. Click **Update**.
   QTS starts updating the network expansion card firmware.
   After the firmware is updated, a restart confirmation window appears.
4. Click **Restart**.

QTS restarts the device to apply the network expansion card firmware changes.

11. Network & File Services

About Network & File Services

The Network & File Services utility allows QTS users to configure and control network and file protocols over a LAN or WAN connection. You can access shared resources over file sharing services and also handle data transfer using various file transfer protocols.

Network administrators can enable multiple protocols for clients to perform remote file editing functions over a web server and allow clients to automatically create a network of devices without manual configuration using service discovery protocols.

QNAP service ports

QNAP uses designated ports for communication. These ports are assigned to a specific service and users must manually open the required ports by adding the port number.

> **Note**
> For these services to operate correctly, their ports should remain open. This may require additional configuration of your firewall or router.

Backup Service

Service	Default Port	Protocol
Rsync	873	TCP
RTRR	8899	TCP

Download

Service	Default Port	Protocol
BitTorrent	6681-6999	TCP/UDP

File Transfers

Service	Default Port	Protocol
AFP	548	TCP
Netbios/SAMBA	137, 138, 139, 445	139, 445(TCP/UDP), 137, 138(UDP)

Service	Default Port	Protocol
FTP/FTPES	20 and 21	TCP
NFS	2049, 111, dynamic ports	TCP/UDP
TFTP	69	UDP

Multimedia

Service	Default Port	Protocol
Twonkymedia	9000	TCP/UDP
UPnP Internet Gateway Device daemon	49152	TCP/UDP

Q'center

Service	Default Port	Protocol
Q'center Server	6600, 6606	TCP/UDP
Q'center Client NAS	6600, 6621, 6623	TCP/UDP

Qsync

Service	Default Port	Protocol
NAS Web	8080	TCP
NAS Web (HTTPS)	443	TCP

System Management

Service	Default Port	Protocol
LDAP Server	389	TCP
MySQL	3306	TCP
SNMP	161	TCP/UDP
SMTP	25	TCP

Service	Default Port	Protocol
Syslog	514	TCP/UDP
Telnet	13131	TCP
SSH/SFTP Server	22	TCP

Virtualization Station

Service	Default Port	Protocol
Virtualization Station	8088	TCP
Virtualization Station (HTTPS)	8089	TCP

VPN

Service	Default Port	Protocol
QVPN (OpenVPN)	1194	UDP
QVPN (PPTP Server)	1723	TCP
QVPN (L2TP/IPSec Server)	500, 4500, 1701	UDP
QVPN (QBelt Server)	443	UDP

Web

Service	Default Port	Protocol
NAS Web	8080	TCP
NAS Web (HTTPS)	443	TCP
Web Server (HTTP, HTTPS)	80, 8081	TCP

Network access settings

QTS users can use network access settings to connect applications to supported services using service binding and securely route traffic between networks using proxy and reverse proxy servers.

Configuring service binding settings

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.

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**.

Network & File Services saves the service binding settings.

Configuring proxy server settings

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.

Important

Prior to enabling the proxy server, ensure that Web Server is enabled in **Control Panel** > **Services** > **Applications** > **Web Server**.

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**.

Network & File Services saves the proxy server settings.

Configuring reverse proxy rule settings

Reverse proxy settings allow users to forward user or web browser requests to web services, enabling efficient and secure data distribution between users and websites.

> **Note**
> You can add up to 64 reverse proxy rules.

1. Go to **Control Panel** > **Network & File Services** > **Network Access**.
2. Click the **Reverse Proxy** tab.
3. Click **Add**.
   The **Add Reverse Proxy Rule** window appears.
4. Configure the rule settings.
    a. Specify a name for the reverse proxy rule.
    b. Configure the source (client) settings.
        1. Select a connection protocol from the following:
            - **HTTP**: Select to establish an unencrypted connection with the website.
            - **HTTPS**: Select to establish an encrypted connection with the website.
              Select **Enable HTTP Strict Transport Security (HSTS)** to advertise to clients that the device accepts only HTTPS requests.
        2. Specify a fully-qualified domain name (FQDN).

            > **Note**
            > You can only specify one domain name for each reverse proxy rule.

        3. Specify a port number for the reverse proxy port to record HTTP or HTTPS traffic.
        4. Select an access control profile from the following:
            - **Allow all connections**

- **Use existing profile**: Select an existing access control profile.
- **Create a new profile**: Select to create a new access control profile.
  1. Specify the access control permission.
  2. Click **Add**.
     The **Add Access Control Rule** window appears.
  3. Select the IP address type.
     - **Single IP address**
     - **CIDR**: Specify an IP address with the subnet mask in CIDR notation.
       Example: 192.0. 1.0/24
  4. Click **Add**.

c. Configure the destination (server) settings.

1. Select a destination protocol.
   - **HTTP**
   - **HTTPS**
   - **HTTP and WebSocket**: Select to allow bidirectional data transfer between the server and client.
   - **HTTPS and WebSocket Secure**: Select to establish a secure bidirectional data transfer using WebSockets over SSL/TLS protocol.
2. Specify the destination hostname.
3. Specify the destination port number.

5. Configure the advanced settings.

a. Click **Edit**.

b. Specify the proxy connection timeout in seconds.

c. Configure header values.

1. Specify a custom header name to include in generated server responses.

   Important
   You cannot repeat header names.

2. Specify the custom header macro value to define the custom response.
3. Select the direction to append the header.

6. Click **Apply**.

Network & File Services saves the reverse proxy settings.

Modifying reverse proxy rules

1. Go to **Control Panel** > **Network & File Services** > **Network Access**.
2. Click the **Reverse Proxy** tab.
3. Perform the following tasks on configured reverse proxy rules.

Task	User Action
Delete a reverse proxy rule	**a.** Beside the reverse proxy rule name, select the checkbox. **Tip** You can select multiple rules. **b.** Click **Delete**. A confirmation message appears. **c.** Click **OK**.
Edit a reverse proxy rule	**a.** Identify a reverse proxy rule. **b.** User Action, select  . The **Edit Reverse Proxy Rule** window appears. **c.** Configure the rule settings. **Note** For details, see Configuring reverse proxy rule settings **d.** Click **Apply**.
Enable a reverse proxy rule	**a.** Beside the reverse proxy rule name, select the checkbox. **Tip** You can select multiple rules. **b.** Click **Enable**.

Task	User Action
Disable a reverse proxy rule	**a.** Beside the reverse proxy rule name, select the checkbox. **Tip** You can select multiple rules. **b.** Click **Disable**.

Network protocol settings

Network protocols enable QTS users to remotely access network devices over the internet or a TCP/IP network. These protocols can be used to map, manage, and monitor network performance and notify users during events of network warnings, failures, bottlenecks, and other events.

Configuring telnet connections

Telnet is a network protocol used to provide a command line interface for communicating with the NAS.

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**.

Network & File Services saves the Telnet settings.

Configuring SSH connections

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 file system. SFTP can be enabled after allowing SSH connections on the NAS.

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**.

Network & File Services updates the SSH connection settings.

Editing SSH access permissions

1. Go to **Control Panel** > **Network & File Services** > **Telnet/SSH**.
2. Click **Edit Access Permission**.
   The **Edit Access Permission** window opens.
3. Select user accounts to give access permissions.

   Important
   Only administrator accounts can log in using an SSH connection.
4. Click **Apply**.

Network & File Services updates the SSH access permissions.

Configuring SNMP settings

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).

1. Go to **Control Panel** > **Network & File Services** > **SNMP**.
2. Select **Enable SNMP Service**.

3. 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 when NAS features or applications fail to be enabled or updated.
Trap Address	Specify the IP addresses of the NMS. You can specify a maximum of three trap addresses.

4. Select an SNMP version for the NMS.

   - **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.
   - **SNMP V3**: Specify the username, authentication protocol and password, and privacy protocol and password.

     1. 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 " ' / \

     2. Optional:
        Select **Use Authentication**.

a. 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**.

b. Specify an authentication password that contains 8 to 64 ASCII characters.

3. Optional:
   Select **Use Privacy**.

   a. Specify a privacy password that contains 8 to 64 ASCII characters.

5. Click **Apply**.

QTS saves the SNMP settings.

Downloading the SNMP 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.

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 1.3.6.1.4.1.24681.2.

1. Go to **Control Panel** > **Network & File Services** > **SNMP**.
2. Under **SNMP MIB**, click **Download**.
   QTS downloads the NAS.mib file to your computer.

File sharing protocol settings

File sharing protocols allows users to access shared resources on a server that supports the file sharing protocol of each client. Shared file access is implemented over local area network (LAN) service and implements automatic synchronization of folder information whenever a folder is changed on the server.

Configuring Samba (Microsoft networking) settings

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.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **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 should 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. Optional: Configure the SMB multichannel settings.

   a. Select **Enable SMB Multichannel**.

   b. Click **SMB Multichannel Settings**.
   The **SMB Multichannel Settings** window opens.

   c. Configure the settings.

Setting	Action
Automatic	Select to allow the system to automatically select multiple network adapters that possess similar configurations.
Manual	Select to manually choose two or more network adapters that have the same network speed.

d. Click **Apply**.
A confirmation window opens.

e. Click **Yes**.

QTS enables SMB multichannel on the device.

6. Optional: Click **Advanced Options**.
The **Advanced Options** window opens.

7. Configure any of the following settings.

a. Select **Enable WINS server** to run a WINS server on the NAS.

b. Select **Use the specified WINS server** to specify a WINS server IP address that QTS will use for name resolution.

c. Select **Local master browser** 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.

> **Important**
> To use the NAS as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".

d. Select **Allow only NTLMv2 authentication** to authenticate clients using only NT LAN Manager Security Support Provider.
When this option is deselected, QTS uses NT LAN Manager (NTLM).

e. 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.

f. Select **Alternative login style** 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.

g. Select **Automatically register in DNS** 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.

h. Select **Enable trusted domains** to join users from trusted AD domains.
This option is only available if AD authentication is enabled.

i. Select **Enable Asynchronous I/O** 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.

j. Select **Enable WS-Discovery to help SMB clients discover the NAS** to enable Web Services Dynamic Discovery (WS-Discovery).
WS-Discovery makes the NAS visible in File Explorer on Windows 10 computers.

k. 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 SMB 3.1 and SMB 3.1.1.

l. 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 SMB 3 will also include SMB 3.1 and SMB 3.1.1.

m. Select **Enable kernel-mode SMB daemon** to increase read/write performance.

> **Important**
> Enabling this option disables SMB encryption for shared folders.

n. Select **Allow Symbolic links within a shared folder** to allow symbolic links within shared folders.

> **Important**
> You must enable this setting in order to restore files from snapshots on Windows using Windows Previous Versions. For details, see Snapshot Data Recovery.

o. Select **Allow Symbolic links between different shared folders** to allow symbolic links between shared folders.

> **Note**
> This setting requires **Allow Symbolic links within a shared folder** to be selected first.

p. Select **Restrict anonymous users from accessing SMB shared folders** to enable user login before accessing SMB shared folders.

> **Note**
> This setting will be locked to **Enabled (strict)** if ABSE is enabled on any shared folder.

q. Select **Veto files** to hide files from users accessing the NAS via SMB.
Files are hidden if their filename matches a pattern in the veto criteria file.

r. Specify the veto criteria for hiding files from SMB NAS users.

> **Note**
> This option is only available when **Veto files** is selected.

s. Select a server signing option to secure message transmissions and prevent relay attacks.

- **Sign if client agrees**
- **Enforce signing**
- **Sign according to selected SMB version**

t. Click **Apply**.
The **Advanced Options** window closes.

8. Click **Apply**.

Network & File Services saves the Samba settings.

Configuring AFP (Apple networking) settings

The Apple Filing Protocol (AFP) is a file service protocol that allows data to be accessed from a macOS device and supports many unique macOS attributes that are not supported by other protocols.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **Apple Networking**.
2. Select **Enable AFP (Apple Filing Protocol)**.
3. Optional: Select **DHX2 authentication support**.
4. Click **Apply**.

Network & File Services saves the AFP settings.

Configuring NFS service settings

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.

The NFS service supports the following permissions in the NFS host access settings. You can apply these permissions to shared folders in **Control Panel** > **Privilege** > **Shared Folders** > **Edit Shared Folder Permissions**, and then selecting **NFS host access** as the permission type.

Permission	Status	Description
sync	Disabled	Disabling **sync** allows the NFS server to override the NFS protocol and reply to requests before any changes made by that request are committed to stable storage. This option usually improves performance.
	Enabled	• **wdelay**: Causes the NFS server to delay writing to the disk to accommodate requests committed to stable storage. • **no wdelay**: Turns off the delay behavior if an NFS server received mainly small unrelated requests. The default can be explicitly requested with the wdelay option.
secure	Disabled	Disabling **secure** requires that requests originate on TCP/IP ports above 1024.
	Enabled	Enabling **secure** requires that requests originate on TCP/IP ports between 1-1024.
Security	Enabled	The transparent file sharing system offered by NFS exposes the data to several security vulnerabilities. The security mechanism allows safe network transmission over trusted networks. NFS protocol provides the following security options to enable secure data transfer between the server and the client. • **sys**: sys or AUTH_SYS is the default unencrypted NFS version 3 security mechanism • **krb5**: Use Kerberos for authentication only. • **krb5i**: Use Kerberos for authentication, and include a hash with each transaction to ensure data integrity. Traffic can still be intercepted and examined, but modifications to the traffic are made apparent. • **krb5p**: Use Kerberos for authentication, and encrypt all traffic between the client and server. This authentication is the most secure mechanism but also incurs the most load. **Note** To use Kerberos-based authentication for NFS shared folders, NFS client and host should join the same AD (Active Directory) server and mount the shared folder via NFSv4 or later versions.

Permission	Status	Description
Squash	Enabled	Remote root users can change any file on the shared file system and expose other users to executable Trojan-infected applications. The squash permission enables the NFS server to transfer the client root role and prevent possible security threats. • **Squash root users**: Maps the remote root user identity to a single anonymous identity and denies the user special access rights on the specified host. • **Squash all users**: Maps all the client requests to a single anonymous identity on the NFS server. • **Squash no users**: The default option does not transfer the client root role.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **NFS Service**.
2. Enable NFS Service.
   a. Select **Enable Network File System (NFS) service**.
   b. Select one or more NFS versions.
   c. Optional: Click **Advanced Options**.
   d. Optional: Select **Use fixed NFS service ports**.

Service	Description
Remote quota server (RQUOTAD_PORT)	Provides information about local user and user group quotas to remote users.
Lock request on TCP port (LOCKD_TCP_PORT)	Applies the Network Lock Manager (NLM) protocol on both TCP clients and servers.
Lock request on UDP port (LOCKD_UDP_PORT)	Applies the Network Lock Manager (NLM) protocol on both UDP clients and servers.
Mount daemon (MOUNTD_PORT)	Monitors and processes `MOUNT` requests from NFSv3 clients.
NSM service daemon (STATD_PORT)	Applies the Network Status Monitor (NSM) Remote Procedure Call (RPC) protocol to inform NFS clients when the NFS server restarts.

Note
Make sure to use different port numbers for each NFS service port.

3. Optional: Select **Enable manage-gids**.

   Tip
   Enable to increase the default maximum number of groups a user can belong to. This option replaces the list of group IDs (GIDs) received from the client with a list of GIDs mapped to the user ID (UID) that can access NFS share if the appropriate client UID also exists in the NAS.

4. Optional: Select **Force client umask**.
   Umask assigns default permissions for new and existing files and folders.

5. Click **Apply**.

Network & File Services saves the NFS service settings.

Accessing FTP (QuFTP Service) settings

QuFTP Service is the QTS File Transfer Protocol (FTP) application that you can access through Network & File Services.

1. Go to **Control Panel** > **Network & File Services**.
2. Click **QuFTP Service**.

QTS opens the QuFTP Service application.

Note
To use this feature, install QuFTP Service from App Center. For more information on QuFTP Service, go to the QNAP website.

Configuring WebDAV settings

The Web Distributed Authoring and Versioning (WebDAV) protocol allows you to share, copy, move and edit remote content on the web.

1. Log on to QTS as administrator.
2. Go to **Control Panel** > **Network & File Services** > **Win/MAC/NFS/WebDAV** > **WebDAV**.
3. Select **Enable WebDAV**.
4. Select one of the following options.
   - **Shared folder permission**
   - **WebDAV permission**
5. Optional: Configure the WebDAV port number settings.

Setting	User Action

Dedicated port number	Manually specify the port numbers for unencrypted (HTTP) and encrypted (HTTPS) connections. • **HTTP port number** • **HTTPS port number**
Web server port number	Select to use the default WebDAV port numbers.

6. Click **Apply**.

Network & Virtual Switch enables WebDAV and saves the settings.

Mounting a shared folder using WebDAV on Windows

Important
Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see Configuring WebDAV settings.

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Windows computer as a network drive via WebDAV.

1. On your Windows computer, open File Explorer.
2. Right-click **This PC** and select **Map network drive**.
   Map Network Drive window appears.
3. Specify the path of the shared folder that you want to access.

   Tip
   The shared folder path uses the following format: http://NAS-IP-address: port number/shared-folder-name. For example: `http://172.17.45.155:80/Public`
4. Enable **Reconnect at sign-in** and **Connect using different credentials**.
5. Click **Finish**.
   Windows Security window appears.
6. Specify your NAS login credentials.

7. Click **Connect**.

> **Tip**
> If you cannot connect to the NAS shared folders using WebDAV, see Troubleshooting WebDAV connectivity issues on Windows.

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using Windows File Explorer.

Troubleshooting WebDAV connectivity issues on Windows

If you are unable to connect to the NAS shared folders using WebDAV protocol on a Windows computer, follow the instructions below to modify the basic authentication level.

1. Right click **Start**.
2. Select **Run**.
3. Type `regedit`.
4. Click **OK**.
5. Open **Registry Editor**.
6. Go to **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **WebClient** > **Parameters**.
7. Open **BasicAuthLevel**.
8. Set the value data to `2`.
9. Restart your computer.
10. Try using WebDAV to connect your computer to the NAS shared folder again.

Mounting a shared folder using WebDAV on Mac

> **Important**
> Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see Configuring WebDAV settings.

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Mac as a network drive via WebDAV.

1. On your Mac, go to **Finder** > **Go** > **Connect to Server**.
   The **Connect to Server** window appears.

2. Specify the path of the shared folder that you want to access.

   Tip
   The shared folder path uses the following format: http://NAS-IP-address: port number/ shared-folder-name. For example: `http://172.17.45.155:80/Public`

3. Click **Connect**.
4. Specify your NAS login credentials.
5. Click **Connect**.

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using macOS Finder.

Service discovery settings

Service discovery enables QTS users to automatically detect and locate services on the network. Service discovery uses zero-configuration networking (zeroconf) to create a usable network based on the Internet Protocol Suite (TCP/IP) when devices are interconnected.

Enabling the 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.

1. Go to **Control Panel** > **Network & File Services** > **Service Discovery** > **UPnP Discovery Service**.
2. Select **Enable UPnP Discovery Service**.
3. Click **Apply**.

Network & File Services enables UPnP discovery service.

Enabling the Bonjour discovery service

Bonjour is a networking technology developed by Apple that enables devices on the same local area network to discover and communicate with each other.

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 & File Services enables Bonjour discovery service.

Enabling the Qfinder discovery service

Enabling the Qfinder discovery service allows the Qfinder Pro utility to discover your QNAP device.

1. Go to **Control Panel** > **Network & File Services** > **Service Discovery** > **Qfinder Discovery Service**.
2. Select **Enable Qfinder Discovery Service**.
3. Click **Apply**.

Network & File Services enables Qfinder discovery service.

Recycle Bin management

The Recycle Bin contains files deleted from the device through File Station, FTP settings, or by clients connected using Samba (Microsoft networking).

Configuring the Recycle Bin settings

1. Go to **Control Panel** > **Network & File Services** > **Recycle Bin**.
2. Select **Enable Recycle Bin**.
3. Optional: Configure the 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.

Setting	Description
Exclude these file extensions	Specify which file extensions are excluded from the Recycle Bin. **Important** File types are case insensitive and must be separated by a comma.

4. Click **Apply**.

Deleting all files in the Recycle Bin

1. Go to **Control Panel** > **Network & File Services** > **Recycle Bin**.
2. Click **Empty**.
   A warning message appears.
3. Click **OK**.
   QTS deletes all files from the Recycle Bin.

Restricting access to the 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 recycle bin**.
5. Select **Restrict the access to Recycle Bin to administrators only for now**.
6. Click **OK**.

12. myQNAPcloud

myQNAPcloud is a service that allows you to access, manage, and share files stored on your QNAP devices remotely through the internet.

Initial setup

Before using the myQNAPcloud service, you must create a QNAP ID and then configure required settings using your QNAP ID.

You can also join the NAS to an organization to allow remote access and management of the device via AMIZ Cloud, a central cloud management platform designed for QNAP devices.

Creating a QNAP ID

QNAP ID allows you to manage your QNAP devices and services. You can create a QNAP ID by using your email address, phone number, or social media account.

Creating a QNAP ID

1. Go to https://account.qnap.com.
   The **QNAP Account** login page appears.
2. Click **Create Account**.
   The **Create Account** screen appears.
3. Specify a nickname, a valid email address or phone number, and a password.
4. Read and acknowledge the Terms of Service and Privacy Policy.
5. Click **Sign Up**.
   The **Data Privacy Notice** box appears.
6. Read the notice, and then click **I Agree**.
   myQNAPcloud sends a verification email or message.
7. Confirm the registration.
   Your QNAP ID is activated.

> **Tip**
> The registration link automatically expires in 15 days. You can go to QNAP Account to send a new activation email.

Creating a QNAP ID with social media

1. Go to https://account.qnap.com/.
   The **QNAP Account** login page displays.
2. Click **Create Account**.
   The **Create Account** screen appears.

3. Click **Google** or **Facebook**.
   The **Data Privacy Notice** box appears.
4. Read the notice, and then click **I Agree**.
   myQNAPcloud prompts you to log into the selected account.
5. Complete the account creation wizard.
   Your QNAP ID is created.

Creating an organization

AMIZcloud is a cloud service that allows the administrators of an organization to remotely access, manage, and monitor QNAP devices. To add a device to AMIZcloud for central management, you first need to create an organization in Organization Center.

1. Go to https://organization.qnap.com/.
2. Sign in using your QNAP ID or social media account.
3. Click **Organization**.
4. Click **Create Organization**.
5. Specify the organization information.
   a. Specify the organization name.
   b. Select a country from the list.
   c. Select the approximate number of members in your organization.
   d. Optional: Specify the website URL.
   e. Optional: Specify a contact number.
6. Click **Next**.
7. Optional: Create a group.
   a. Click **Create Groups**.
   b. Specify the group name.
   c. Optional: Add a description.
   d. Click **Create**.
8. Click **Next**.
9. Optional: Invite administrators.
   When you create an organization, you are automatically assigned as an administrator.
   a. Click **Invite Administrators**.
   b. Specify an email address associated with a QNAP ID.
   c. Optional: Select a group.
   d. Optional: Add a description.

e. Click **Add**.

> **Tip**
> You can invite multiple administrators at a time.

f. Click **Done**.
myQNAPcloud sends an invitation email or message.

The organization is created and added to the **Organization** dashboard. Administrator can also create sites for different locations of your organization. You can select a site when registering a new device.

Setting up myQNAPcloud and AMIZ Cloud for the NAS

myQNAPcloud allows you to remotely access the NAS via the Internet and to access various QNAP cloud services. To start using myQNAPcloud, you should first sign in with your QNAP ID and then set up the service for your device. You can also choose to add your device to an organization, so that organization administrators can remotely manage this device via AMIZcloud.

1. Open myQNAPcloud.
2. Enter your QNAP ID and password.
3. Click **Sign In**.
4. Specify a device name.

> **Tip**
> myQNAPcloud creates a SmartURL using the device name that you specify. You can also choose to reuse an existing device name that you have created for another device.

5. Optional: Join the NAS to an organization.

> **Tip**
> This allows the administrators of this organization to access, manage, and monitor this device via AMIZcloud.

a. Select an organization.
b. Select a site.
c. Click **Next**.

d. Enable AMIZ Cloud Agent.

Note

- AMIZ Cloud Agent is a utility that communicates with AMIZcloud and collects the data of various resources on your device for analytics purposes without any identifiable person information. This helps you better monitor your device status.
- myQNAPcloud automatically enables AMIZcloud when you add the device to an organization for central management.

6. Click **Next**.
7. Enable remote access services.

Service	Description
myQNAPcloud Link	This service allows you to remotely access your device via QNAP mobile apps, desktop utilities, and the myQNAPcloud website. myQNAPcloud automatically enables myQNAPcloud Link when you add the device to an organization for central management. If you choose not to join the NAS to an organization, you have to configure access control settings to decide which users can access your device. • **Private**: Only you can access your device. • **Public**: All users can find and access your device. • **Customized**: Only invited users can access your device. For details, see Configuring device access controls for stand-alone devices.
DDNS	This service automatically maps a domain name to the dynamic IP address of your device. Users can always connect to your device using the same URL without knowing the current IP address. You can configure DDNS settings later after finishing this setup. For details, see Configuring DDNS settings.

8. Click **Apply**.

The system configures the NAS according to your settings. If you do not add the device to an organization during the setup, you can do so later by signing out and then signing in again with your QNAP ID to open the setup wizard.

Basic operations and service statuses

You can perform basic operations and monitor the status of each myQNAPcloud service on the **Overview** screen. The list of available services varies depending on the selected mode.

Basic Operations

Icon	User Action
	Click to open the AMIZcloud Portal. The AMIZcloud Portal provides a central management platform for QNAP devices. **Note** This icon is only available if you have added this device to an organization.
	• Organization device: Click to switch between organizations. • Stand-alone device: Click to switch between QNAP IDs.
	Click to sign out of myQNAPcloud. You can then sign in with another QNAP ID. Or you can sign in again with the same QNAP ID but use other settings during the setup.
	Click to modify the device name.
	Click to copy the SmartURL.

Service Status

Status	Description
Normal	This service is connected to both the internet and the cloud server.
Abnormal	This service is connected to the internet but is unable to connect to the cloud server.
Enabled	This service is enabled and functioning properly.
Disabled	This service is disabled.
Not Installed	This service is not yet installed.
Disconnected	This service cannot connect to the Internet.

Access management

myQNAPcloud allows you to configure settings and manage services designed to facilitate remote access and ensure secure connection.

Configuring device access controls for stand-alone devices

You can configure device access controls to decide whether your devices and services are accessible to other users. If you choose not to add your device to an organization, you can choose one of the following access modes in myQNAPcloud to define your device accessibility.

1. Log in to the NAS.
2. Open myQNAPcloud.
3. Go to **Access Control**.
4. Select an access control option.

Mode	Description	User Action
Public	All users can search for your device and view the published services on the myQNAPcloud website.	Select **Public**.
Private	Your device does not appear in search results. Only you can access your device on the myQNAPcloud website.	Select **Private**.
Customized	Your device is visible only to yourself and users you have invited. Others users cannot access even with a SmartURL.	**a.** Select **Customized**. **b.** Invite users. 1. Click  . 2. Specify the user's email address or phone number. 3. Click **Save**. **c.** Enable any services to publish for invited users.

Configuring device access controls for organization devices

If you add your device to an organization, you can choose an access mode on the myQNAPcloud web portal to determine which organization administrators can access and manage the device.

1. Go to https://www.myqnapcloud.com.
2. Sign in with your QNAP ID.
3. Go to **Device Management** > **Organization Devices**.
4. Select an organization and a site.
5. Click a device.

6. Go to **Access Control**.
7. Select one of the following options.

Option	Description
All Administrators	All administrators in this organization can access and manage devices with their QNAP ID via myQNAPcloud, AMIZcloud, and other cloud services.
Specific Administrators	Only you and specific members or groups in this organization can access and manage devices. This applies to all QNAP cloud services that require device management permissions. You can edit the user/group list to grant or deny access permissions.

Enabling myQNAPcloud Link

Important
myQNAPcloud Link cannot be disabled when the device is added to an organization.

1. Open myQNAPcloud.
2. Go to **myQNAPcloud Link**.
3. Enable **myQNAPcloud Link**.

Tip
If there are issues with the connection, click **Reconnect**.

Restoring the AMIZ Cloud Agent connection

This service is enabled by default. If there are issues with the connection, complete the following steps.

Important
AMIZ Cloud Agent is only available when the device is added to an organization.

1. Open myQNAPcloud.
2. Go to **AMIZ Cloud Agent**.
3. Click **Reconnect**.

Configuring DDNS settings

myQNAPcloud provides DDNS service to map domain names to dynamic IP addresses. This helps you simply your connection to the device.

1. Open myQNAPcloud.
2. Go to **DDNS**.
3. Enable **My DDNS**.
4. Perform any of the following tasks.

Task	User Action
Change the myQNAPcloud DDNS domain name	**a.** Click  . The **Change Device Name Wizard** appears. **b.** Specify a device name containing up to 30 alphanumeric characters. **c.** Click **Apply**.
Update myQNAPcloud	Click **Update**.
Manually configure the DDNS IP address	**a.** Click **Settings**. The **Public IP Address** window appears. **b.** Select an option. • **Use WAN interface**: When multiple WAN ports are available, you can select which WAN interface to use for monitoring IP changes. • **Assign static IP addresses**: myQNAPcloud binds the DDNS to the specified static IP address regardless of changes to the network environment. • **Automatically obtain IP address**: myQNAPcloud automatically detects the WAN IP. **c.** Click **Apply**.

Configuring UPnP port forwarding

UPnP allows your devices to automatically configure port forwarding settings and discover other devices on the network. Port forwarding is only available if your router supports UPnP.

Warning
Despite its convenience, UPnP may expose your device to public networks. This may allow malicious attackers to access your sensitive data, scan your private networks, and use your devices for DDoS attacks. To ensure your device and data security, we recommend disabling UPnP and manually configuring port forwarding settings on your router.

1. Open myQNAPcloud.

2. Click  on the top-right corner.
3. Select **Auto Router Configuration**.
   A confirmation message appears.
4. Read the instructions carefully and understand the risks of enabling UPnP.

   Tip

   After enabling UPnP Port Forwarding, you still have to manually open ports. In addition, every time you disable UPnP, myQNAPcloud automatically disables all ports and services that you had enabled. If you enable UPnP again, you will need to manually enable these ports and services again. This measure is to minimize your exposure to potential cyber attack.

5. Click **OK**.
6. Enable **UPnP Port Forwarding**.
   Your device scans for UPnP routers on the network.

   Tip

   - You can go to **Overview** to verify that there are no connectivity errors.
   - If your device cannot locate the router, click **Rescan**. If the issue persists, click **Diagnostics**, and then verify your network configuration or contact QNAP support through **Helpdesk**.

7. Optional: Add a new service to the **Forwarded Services** table.
   a. Click **Add NAS Service**.
      The **Add NAS Service** window appears.
   b. Specify a NAS service name that contains 1 to 64 ASCII characters.
   c. Specify a port number.
   d. Select an external port setting.
      - **Automatic**: myQNAPcloud automatically selects an available external port.
      - **Manual**: You can specify a new port if the current service port is being used by other services.
   e. Select a protocol.
      If you are unsure about this setting, select **TCP**.
   f. Click **OK**.
8. In the **Forwarded Services** table, select the services you want to forward.
9. Click **Apply to Router**.

Installing an SSL certificate

Important
myQNAPcloud SSL web service and Let's Encrypt certificates can only be used with the myQNAPcloud domain.

1. Open myQNAPcloud.
2. Go to **SSL Certificate**.
3. Download and install a certificate.

Type	Description	User Action
myQNAPcloud SSL web service certificate	This certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users.	Hover the mouse pointer over **myQNAPcloud** and then click **Download and install**. **Important** To apply the SSL certificate, you must purchase the SSL Certificate License and activate the license in License Center. For QTS users, you can purchase the license from the myQNAPcloud web portal. For QNE users, you can purchase the license from QNAP Software Store. This certificate should match the specified device region. For example, if your device region is set to `Global`, you must purchase a Global Domain license.

Type	Description	User Action
Let's Encrypt certificate	Let's Encrypt is a free, automated, and open certificate authority that issues domain-validated security certificates. You can install Let's Encrypt certificates with the myQNAPcloud DDNS service. You can choose to automatically renew this certificate before it expires. **Tip** Although Let's Encrypt is a free service, you need to renew their certificates every 90 days due to some limitations. We recommend using myQNAPcloud SSL web service certificate.	**a.** Hover the mouse pointer over **myQNAPcloud** and then click **Download and install**. The **Download & Install SSL Certificate** window appears. **b.** Specify a valid email address. This address is required for the Let's Encrypt account registration. **c.** Optional: Select **Automatically renew domain before expiration.** **d.** Click **Confirm**.

myQNAPcloud applies the certificate and displays the details.

Tip
To delete the certificate from the device, click **Remove**.

13. App Center

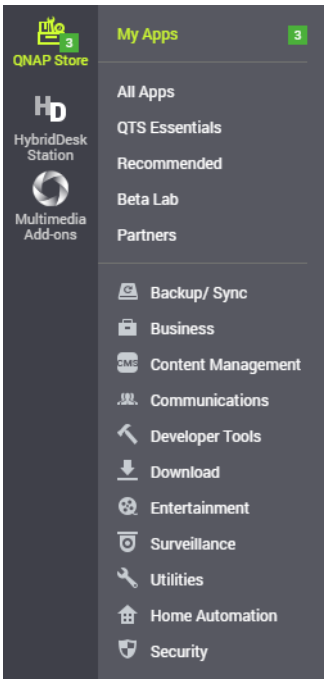
App Center is a digital distribution and management platform in QTS where you can browse, download, and manage applications and utilities developed for the QNAP NAS.

Navigation

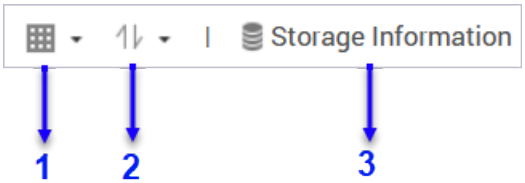
You can view all App Center apps in the left panel or configure a number of settings using the toolbar.

Left panel

The left panel allows you to browse available apps in various categories. You can go to the **My Apps** section to view all your installed apps. App Center displays a badge count to indicate the number of available updates.



Toolbar



Left side

No.	Elements	Possible User Actions
1	View mode	• Click the icon to switch between two view modes. • Click and select a view mode.
2	App sorting	Click and select an app sorting method.
3	Volume information	View the basic volume information and the installation locations of your apps. For more volume information, click **Details**.

Right side

No.	Elements	Possible User Actions
1	Search	Specify keywords to search for apps. App Center instantly displays search results based on specified keywords.
2	Refresh	Reload the data in App Center to view the current status of your apps.
3	Manual installation	Manually install an app by uploading an installation package. For details, see Installing an app manually.
4	Settings	Configure various App Center settings. For details, see App Center Settings.
5	More	View the Quick Start or the Help document for more information about App Center.

App management

The App Center allows you to enable or disable an app, assign CPU resources to load-intensive apps, update apps, and configure app update settings.

Viewing app information

You can browse apps and view their descriptions in the App Center. This helps you decide whether to install or update an app.

1. Open App Center.
2. Locate an app.
3. Click the app icon.
   App Center displays the app information in a new window.
4. Perform one of the following actions.
   - View the app description
   - View the available version of the app
   - View the currently installed version of the app if it is currently installed
   - View the installation date of the app if it is currently installed
   - View the digital signature details
   - View the app changelog
   - Go to the QNAP forum
   - View the app tutorial
   - Download the app installation package

Buying an app license

Important

- Some apps require you to purchase an app license or subscription. You can purchase app licenses or subscriptions in Software Store.
- You must activate a purchased app license to operate a paid app.

1. Open App Center.
2. Locate an app.
3. Click **Buy License**.
   The **Buy License** window opens in a new web page.

   Important
   For details about license subscription or purchasing a license from Software Store, see Licenses.
4. Click **Activate License**.
   The **License Center** window appears.
5. Activate the license.
   For details, see License activation.

6. Click **Next**.
   - The **App Center** window appears.
   - App installation will automatically start in App Center.

Installing an app from App Center

Warning
QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.

Important
- Certain apps require activating a subscription or license before app installation. For details, see Licenses.
- Based on the app you choose to install, App Center may display a confirmation message that provides more information and asks for your approval for installation. Certain apps also require you to specify the installation location. Read the message carefully before installing the app.

1. Open App Center.
2. Locate an app.
3. Optional: Click the app icon to view the app information.
4. Select the app update frequency.
5. Click **Install**.
   The app is installed.

Installing an app manually

Warning
- QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.
- App Center does not allow the installation of invalid apps, including apps with invalid digital signatures, apps not approved by App Center, or from the Software Store. If App Center detects that an app is invalid, it will immediately terminate the app installation and prompt you to remove the app.

Important
Certain apps require activating a subscription or license before app installation. You can go to the Software Store to purchase an app license or subscription. For details about activating an app license, see Licenses.

1. Open App Center.
2. Click  on the toolbar.
3. Click **Install Manually**.
   The **Install Manually** window appears.
4. Click **Browse**.
5. Locate and select the installation package.
6. Click **Install**.
   A message appears.
7. Depending on the scenario, perform one of the following actions.

Scenario	Actions
The app has a valid digital signature.	**a.** Read the confirmation message. **b.** Click **OK**.
The app does not have a valid digital signature, and you enabled the installation of apps without valid digital signatures.	**a.** Read the confirmation message. **b.** Click **OK**.
The app does not have a valid digital signature, and you did not enable the installation of apps without valid digital signatures.	**a.** Read the warning message. **b.** Select **I understand the risks and want to install this application.** **c.** Click **Install**.

Tip
For more information on this setting, see Enabling Installation of Apps without Digital Signatures.

App Center installs the app.

Updating an app

When updates are available for an installed app, App Center moves the app to the **Update** or **Required Update** section based on the importance of updates. You must perform required updates to ensure the functionality, compatibility, and data security of your apps.

1. Open App Center.
2. Locate an app in the **Update** or **Required Update** section.
3. Click **Update** or **Required Update**.
   A confirmation message appears.
4. Click **OK**.

Batch updating multiple apps

1. Open App Center.
2. Perform one of the following updates.

Updates	Action
Only required updates	Below the toolbar, click **Required Update**.
All available updates	Below the toolbar, click **All**.

   A confirmation message appears.
3. Click **OK**.

Enabling or disabling an app

You can enable or disable non-built-in apps in App Center.

Note

- Disabling an app may affect the functionality of other apps.
- Disabling an app does not remove or uninstall the app.

1. Open App Center.
2. Locate an app.
3. Perform one of the following actions.

Action	Steps
Enable the app	Click **Start**.
Disable the app	**a.** Click  . **b.** Select **Stop**.

- After an app is enabled, its action button displays **Open**.

- After an app is disabled, its action button displays **Start**.

Migrating an app

Most installed apps can be migrated to another volume to better allocate system resources. Certain apps, however, must be installed on the system volume and cannot be migrated.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Migrate to**.

   Note
   If this option is unavailable, the app cannot be migrated.

   The **App Migration** window appears.
5. Select the destination volume.
6. Click **Migrate**.
   A confirmation message appears.
7. Click **OK**.

Granting or denying user access to an app

QTS administrators can grant or deny user access to apps. The main menu of non-administrator users only display the apps that they have access to.

1. Open App Center.
2. Locate an app.
3. Click .
4. Hover the cursor over **Display on**.
5. Select one of the following options:
   - Administrator's main menu

     Note
     This is the only available option for many built-in system utilities, which non-administrators cannot be granted access to.
   - Every user's main menu

Uninstalling an app

Warning
Uninstalling an app also deletes the related user data.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Remove**.
   A confirmation message appears.
5. Click **OK**.

Viewing apps installed on other devices

You can view apps that have been installed on other devices. To view apps installed on other devices, myQNAPcloud must be set up on the device, and device must be logged into myQNAPcloud with the same QNAP ID.

1. Open App Center.
2. Click on the toolbar.
3. Click **Apps Installed on All Devices**.
   The **Apps Installed on All Devices** window appears.
4. Next to **myQNAPcloud device name**, select a device.
   All apps on the selected device are displayed.
5. Optional: Install an app.
   a. Select the checkbox next to an app to select it.
   b. Click **Install**.
      The selected app is installed on the current device.

App Center settings

You can configure the app respository, update settings, and enable installation of apps without digital signatures.

Adding an app repository

You can add an app repository to enrich the content in App Center. This allows you to download and install apps from third-party sources.

1. Open App Center.

2. Click ⚙ on the toolbar.
3. Go to **App Repository**.
4. Click **Add**.
   The **Add** window appears.
5. Specify the following connection information.
   - Name
   - URL
6. Optional: Specify the login credentials.
   - Username
   - Password
7. Click **Add**.

App Center adds the repository to the list. You can select the repository and then click **Edit** to modify its settings or click **Delete** to remove this repository from App Center.

Configuring app update settings

Important
By default, QTS checks for available app updates on a regular basis. To ensure maximum system security and performance, QNAP recommends updating apps when updates are available.

1. Open App Center.
2. Click ⚙.
3. Go to **Update**.
4. Go to **When updates are available, I want to** and select one of the following options:

Option	Description
Send a notification	QTS sends notifications when updates are available for your apps. Click **Create Notification Rule** to create rules in Notification Center. For details, see Notification Center.
Install all updates automatically	App Center automatically installs all available updates for your apps.

Option	Description
Install all required updates automatically	App Center automatically installs all required updates for your apps to ensure their functionality, compatibility, and data security.

5. Go to **Update/Notification time** and specify when App Center sends notifications for or installs app updates.

   Note
   App updates are installed within one hour of the specified time.

6. Click **Apply**.

Digital signatures

QNAP uses digital signatures to validate apps created by QNAP or QNAP-trusted publishers. The use of digital signatures prevent the unauthorized tampering of apps that may lead to security risks.

A digital signature is considered valid if it meets the following criteria.

- The digital signature has not been tampered with.
- The digital signature has not expired.
- The digital signature is certified by QNAP.

Enabling installation of apps without digital signatures

Warning

- A valid digital signature ensures that an application was created by QNAP or a QNAP-trusted publisher. It also ensures that the app has not been maliciously tampered with. Installing apps without valid digital signatures may expose your NAS to security risks. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of such apps.
- App Center never installs apps with invalid digital signatures even if this setting is enabled.
- Installation of apps without digital signatures is disabled by default in **Settings**.

1. Open App Center.
2. Click  on the toolbar.
   The **Settings** window appears.
3. Go to **General**.

4. Select **Allow installation and execution of applications without a digital signature**.

   Important
   App Center does not allow the installation of apps with tampered digital signatures even when this setting is enabled.

5. Click **Apply**.

14. Licenses

QNAP licenses enable users to gain access to certain advanced features or premium products. This chapter introduces important concepts and demonstrate essential tasks to help you start using QNAP licenses.

About QNAP licenses

QNAP offers a wide variety of licenses. Some basic licenses are provided free of charge. You can purchase premium licenses to further enhance the functionality of your QNAP products. QNAP also provides multiple management portals, flexible subscription plans, and various activation options to meet your different needs.

License types and plans

The licensing mechanisms and available plans of QNAP licenses vary depending on corresponding software products. They can be divided into the following categories.

License Types

License Types	Description
Device-based	• Allows users to use a software product installed on hardware devices, such as applications. • Multi-seat licenses can be activated and used on multiple devices.
Floating	• Allows users to use a software product in the cloud or on a virtual platform, such as QuTScloud and applications in QuTScloud. • Can be activated and used on a limited number of devices at a time
User-based	• Allows a limited number of authorized users to access a web-based service, such as Qmiix.

License Plans

License Plans	Description
Subscription	Authorizes users to use a software product with a recurring monthly or annual fee
Perpetual	Authorizes users to use a software product indefinitely
One-time	Authorizes users to use a software product within a predefined period of time

Validity period

The validity period of a QNAP subscription-based license starts from the date of purchase, not from the date of activation.

For example, if a user starts the subscription of an annual license on January 1, 2020, the next billing date will be January 1, 2021, regardless of the date of activation. If the user cancels the subscription, the license will still remain valid until January 1, 2021.

If the user unsubscribes from a license but subscribes to the same product later, the validity period and billing cycle will begin from the date of the new subscription.

License portals and utility

Portal	Description	URL
QNAP Software Store	The QNAP Software Store is a one-stop shop where you can purchase licenses for QNAP and QNAP-affiliated software.	https://software.qnap.com
QNAP License Center	The QNAP License Center allows you to monitor and manage licenses of applications running on your local device.	-
QNAP License Manager	QNAP License Manager is a portal that allows you and your organizations to remotely activate and manage licenses under your QNAP ID.	https://license.qnap.com
Old QNAP License Store	Users of QTS 4.3.4 (or earlier) can purchase licenses from this online store.	https://license2.qnap.com

Software Store

Software Store allows you to purchase licenses for applications. Through Software Store, you can perform the following actions.

- Purchase or upgrade licenses
- Manage your account information
- View purchased subscriptions
- Cancel your subscriptions
- Request a refund for your orders

License Center

License Center allows you to monitor and manage the licenses of your applications running on your local device. Through License Center, you can perform the following actions.

- Activate and deactivate licenses either online or offline
- Remove licenses from the local device
- Recover licenses if your device is reset, reinitialized, or restored to factory default
- Transfer licenses purchased from the old QNAP License Store to the new QNAP License Manager

License Manager

License Manager is a portal that allows you to manage all licenses under QNAP IDs and organizations. Through License Manager, you can perform the following actions.

- View details of your licenses
- Activate and deactivate licenses
- Assign a user-based license to a QNAP ID

> **Important**
> To remotely activate or deactivate licenses, you must enable myQNAPcloud Link on your QNAP device.

Buying a license using QNAP ID

Before buying a license, ensure the following.

- The application is already installed on your device.
- You are signed in to myQNAPcloud.

1. Go to https://software.qnap.com.
2. Sign in with your QNAP ID.
3. Locate the product on the list, and then click **Buy** or **Subscribe Now**.
   The license details appear.
4. Select a license, and then review the price.
5. Click **Checkout Now**.

   > **Tip**
   > You can also click **Add to Cart** and then continue shopping.

   The purchase summary page appears in your web browser.

6. Select a payment method.

Payment Method	User Action
Credit card	**a.** Specify your card information. **b.** Verify the items and the price on the order. **c.** Agree to QNAP terms and conditions. **d.** Click **Place Order**.
PayPal	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Pay with PayPal** PayPal authentication window appears. **d.** Specify your PayPal login credentials. **e.** Click **Next**. **f.** Follow PayPal instructions to complete the payment.
Google Pay	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Buy with Google Pay**. Google Pay authentication window appears. **d.** Follow Google Pay instructions to complete the payment.

After the payment, you can view order details in **My Orders** and manage your subscriptions in **My Subscriptions**.

You can activate your license right after the purchase or at a later time.

For details, see License activation.

License activation

You need to activate purchased licenses to access features provided by the license. You can activate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through Software Store are stored in your QNAP ID account. They can be accessed through both License Center and the QNAP License Manager website.

Activation Method	Description
Using a license key	You can generate the 25-character license key after purchasing licenses through the QNAP Software 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 license key.
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 key or PAK.
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. For details, see Activating a license using a product key or PAK.
Offline	Use this method when the device 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 device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can activate their licenses using QNAP ID in either Qfinder Pro, License Center, or License Manager.

- Activate your license using one of the following methods.

Method	Steps
Qfinder Pro	Qfinder Pro allows you to discover QNAP devices on your local network. **a.** Open Qfinder Pro on your computer. **Tip** You can download Qfinder Pro from the QNAP website. **b.** Select your device form the list. **c.** Right-click the device and select **License Activation**. **d.** Specify your device username and password. The **License Activation** windows appears. **e.** Select **Activate with QNAP ID**. **f.** Click **Select License**. **g.** Specify your QNAP ID and password. **h.** Click **Select License**. **i.** Select a license from the list. **j.** Click **Activate**. License Server activates the license. A confirmation message appears. **k.** Click **Close**. The license is activated for the device.

Method	Steps
License Center	**a.** Open License Center. **b.** Go to **My Licenses**. **c.** Click **Activate License**. The **License Activation** window appears. **d.** Select **Activate with QNAP ID**. **e.** Click **Select License**. **f.** Select a license from the list. **Tip** If you select a multi-seat license, you can specify the number of seats that you want to activate. **g.** Click **Add**. License Center activates the license. A confirmation message appears. **h.** Click **Close**. The license appears on the list of active licenses.
License Manager	**a.** Open your web browser. **b.** Go to https://license.qnap.com. **c.** Sign in with your QNAP ID. **d.** Locate a license from the license list. **e.** Click  . The **Activate License** window appears. **f.** Select **Online Activation**. **g.** Select a device. **h.** Specify your credentials on the device. **i.** Click **Allow**. A confirmation message appears. **j.** Click **OK**. License Manager activates the license. **k.** Click **Close**. The license appears on the list of active licenses.

Activating a license using a license key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID.

You can activate a license using a license key. After purchasing a license from QNAP Software Store, you can generate a license key from the License Manager website and apply the key in License Center. A license key contains 25 characters and always starts with the letter L.

For details, see Generating a license key.

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
   The **License Activation** window appears.
4. Select **Activate with a License Key**.
5. Specify the key.
6. Read and agree to the terms of service.
7. Click **Verify Key**.
8. Verify the license information.
9. Optional: Specify the number of seats to activate.

   Note
   This option is only available for licenses that support multiple seats.

10. Click **Activate**.
    The license is activated.
    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. From the list of licenses, select the license you want to generate a key for.
5. Click  .
   The **Activate License** window appears.

6. Select **License Key**.
   License Manager generates the license key.

   Tip
   Click **Renew License Key** to generate a new key.
   This renews your license key and protects you from any unauthorized access to your existing license key.

7. Hover the mouse pointer over the license key and click  .
   Your system copies the license.
8. Click **Done**.

The copied license key can be pasted later for license activation.

Activating a license using a product key or PAK

Before activating a license using a product key or a product authorization key (PAK), ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

You can activate a license with a product key or PAK. You may find a product key printed on a physical copy of your product. A product key contains 25 characters and always starts with the letter P.

On the other hand, you may obtain a product authorization key (PAK) if you purchase a license from the old QNAP License Store. A PAK contains 24 digits of random numbers.

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
4. The **License Activation** window appears.
5. Select **Activate with a Product Key or PAK**.
6. Specify the key.
7. Read and agree to the terms of service.
8. Click **Verify Key**.
9. Verify the license information.
10. Click **Activate**.
    The license is activated.
    A confirmation message appears.
11. Click **Close**.
    The license appears on the list of active licenses.

Activating a license offline

You can activate your license offline if your QNAP device is not connected to the Internet. You first need to generate a device identity file (DIF) from Qfinder Pro or from License Center on your device and then upload the DIF to License Manager in exchange for the license install file (LIF). You can then activate the license using the LIF in Qfinder Pro or in License Center on your device.

1. Choose one of the following methods.

Methods	User Action
Offline activation using Qfinder Pro	Qfinder Pro allows you to discover QNAP devices on your local network. **a.** Open Qfinder Pro on your computer. **Tip** You can download Qfinder Pro from the QNAP website. **b.** Select your device from the list. **c.** Right-click the device and then select **License Activation**. **d.** Specify your username and password. The **License Activation** window appears. **e.** Select **Offline Activation**.
Offline activation using License Center	**a.** Log in to your QNAP device. **b.** Open License Center. **c.** Go to **My Licenses**. **d.** Click **Activate License**. The **License Activation** window appears. **e.** Select **Offline Activation**.

2. Read and agree to the Terms of Service.
3. Click **Generate Device Identity File**.
Qfinder Pro or License Center downloads the device identity file (DIF) to your computer.
4. Read the instructions and click **Go to License Manager**.
Your web browser opens the **QNAP License Manager** website.
5. Sign in with your QNAP ID.
6. From the list of licenses, select the license you want to activate.
7. Click **(Upload Device Identity File)**.
The **Activate License** window appears.

8. Click **Browse**.
   The file browser appears.
9. Locate and select the DIF from your computer.
10. Click **Upload**.
    A confirmation message appears.
11. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
12. Click **Done**.
13. Go back to Qfinder Pro or License Center.
14. In the **License Activation** window, click **Upload License File**.
15. Click **Browse**.
    The file browser appears.
16. Locate and select the LIF from your computer.
17. Click **Import**.
    Qfinder Pro or License Center uploads the LIF and displays the license summary.
18. 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 purchased through Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website To deactivate this type of license, see Deactivating a license using QNAP ID.
Offline	Use this method when the device is not connected to the internet. For details, see Deactivating a license offline.

Deactivating a license using QNAP ID

Before deactivating your license, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can deactivate their licenses using QNAP ID in either License Center or License Manager.

- Deactivate your license using one of the following methods.

Method	Steps
License Center	**a.** Open License Center. **b.** Go to **My Licenses**. **c.** Identify the license you want to deactivate, and then click . The **License Deactivation** window appears. **d.** Select **Use QNAP ID**. **e.** Read and acknowledge the warning. **f.** Click **Deactivate**. A confirmation message appears. **g.** Click **Close**. License Center deactivates the license and removes the license from the list of active licenses.
License Manager	**a.** Open your web browser. **b.** Go to https://license.qnap.com. **c.** Sign in with your QNAP ID. **d.** From the list of licenses, select the license you want to deactivate. **e.** Click . The **Deactivate License** window appears. **f.** Read and acknowledge the warning. **g.** Click **Deactivate**. License Center deactivates the license. A confirmation message appears. **h.** 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. Read the instructions, and then click **Generate License Uninstall File**.
   License Center downloads the license uninstall file (LUF) to your computer.
7. Open your web browser.
8. Go to https://license.qnap.com.
9. Sign in with your QNAP ID.
10. From the list of licenses, select the license you want to deactivate.
11. Under **Advanced Options**, click  .
    The **Deactivate License** window appears.
12. Read and agree to the terms.
13. Click **Offline Deactivation**.
14. Click **Browse**.
    The file browser appears.
15. Locate and select the LUF from your computer.
16. Click **Upload**.
    QNAP License Manager deactivates the license.
    A confirmation message appears.
17. Click **Done**.

License extension

License Center will notify you soon before any of your subscription-based licenses expire. The exact dates vary depending on the type of your licenses (ranging from one week to one month before the expiration date). You can extend your QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through License Center or Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website. 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 device 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.

Activation Method	Description
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 device 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.

Extending a license using QNAP ID

Before extending licenses, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.
- You have an existing valid, unused license.

> **Note**
> Subscription-based licenses will be automatically renewed in License Manager. You cannot manually extend a 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 about to expire, its status is `Expires soon`.

   The **License Extension** window appears.
4. Select **manually extend a license**.
5. Select **Extend offline**.
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 Manager**.
    Your web browser opens the QNAP License Manager website.
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 **Extend**.
    The **Extend License** window appears.
16. Select **Use an unused license**, and then click **Next**.
    The list of unused licenses appears.
17. 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.
18. Click **Next**.
19. Click **Browse**.
    The file browser appears.

20. Locate and select the DIF from your computer.
21. Click **Upload**.
    A confirmation message appears.
22. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
23. Click **Done**.
24. Go back to License Center.
25. In the **License Extension** window, click **Next**.
26. Click **Browse Files**.
    The file browser appears.
27. Locate and select the LIF from your computer.
28. Click **Next**.
    License Center uploads the LIF and displays the license summary.
29. Click **Extend**.
    A confirmation message appears.
30. 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 about to expire, its status is `Expires soon`.

   The **License Extension** window appears.
4. Click **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
   A notification message appears.
8. Click **Download**.
   License Center downloads the device identity file (DIF) file to your computer.
9. Read and agree to the terms of service.
10. Click **Next**.

11. Read the instructions, and then click **Go to License Manager**.
    Your web browser opens the QNAP License Manager website.
12. Sign in with your QNAP ID.
13. Go to **My Licenses**.
14. From the list of licenses, select the license you want to activate.
15. In the table below, click **Activation and Installation**.
    The license activation details appear.
16. Click **Extend**.
    The **Extend License** window appears.
17. Select **Use a product key**, and then click **Next**.
18. Specify the product key.
19. Click **Next**.
    A confirmation message appears.
20. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
21. Click **Done**.
22. Go back to License Center.
23. In the **License Extension** window, click **Next**.
24. Click **Browse Files**.
    The file browser appears.
25. Locate and select the LIF from your computer.
26. Click **Next**.
    License Center uploads the LIF and displays the license summary.
27. Click **Extend**.
    A confirmation message appears.
28. Click **Close**.
    The license appears on the list of active licenses.

Upgrading a license

Before upgrading a license, ensure the following.

- The application is already installed on your device.
- You are signed in to myQNAPcloud.

Users can upgrade their existing basic licenses to premium licenses to gain access to advanced features.

1. Open your web browser.

2. Go to https://software.qnap.com.
3. Click your account name and select **MY ACCOUNT**.
4. Click **Upgrade Plans**.
   A list of upgradable subscriptions is displayed.
5. From the list of subscriptions, find the license you want to upgrade and click **Upgrade**.
   The **Current Plan** window appears.
6. From the list of upgrade plans, select an upgrade and click **Add to Cart**.
7. Click  .
8. Click **GO TO CHECKOUT**.
9. Select a payment method.

Payment Method	User Action
Credit card	**a.** Specify your card information. **b.** Verify the items and the price on the order. **c.** Agree to QNAP terms and conditions. **d.** Click **Place Order**.
PayPal	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Pay with PayPal** PayPal authentication window appears. **d.** Specify your PayPal login credentials. **e.** Click **Next**. **f.** Follow PayPal instructions to complete the payment.
Google Pay	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Buy with Google Pay**. Google Pay authentication window appears. **d.** Follow Google Pay instructions to complete the payment.

10. Apply the license upgrade to your QNAP device.
    a. Open your web browser.
    b. Go to https://license.qnap.com.

c. Sign in with your QNAP ID.

d. Locate the license from the license list.

e. Click  .
The **Activate Upgraded License** window appears.

f. Select **Online Activation**

g. Click **Next**.

h. Specify your credentials on the device.

i. Click **Allow**.
A confirmation message appears.

j. Click **Close**.

The upgraded license is activated.

Viewing license information

1. Open your web browser.
2. Go to https://license.qnap.com.
3. Sign in with your QNAP ID.
4. View the license information using one of the following modes.

Viewing Mode	User Actions
List by Device	This mode displays all the activated licenses on each device. This allows you to quickly view and manage your licenses on a specific device. • Click a device and then click **Device Details** to view the details of the selected device. • Click a device and then click **Activation and Installation** to view the details of your licenses. You can also activate or deactivate licenses.
List by License	This mode displays your purchased licenses and their details, including available seats, license types, validity period, and status. • Click a license and then click **License Details** to view the details. • Click a license and then click **Activation and Installation** to view the details. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file. • Click a license and then click **Usage Record** to view the history of the selected license.

Viewing Mode	User Actions
List by Product	This mode displays your purchased licenses for each product. This allows you to view and manage all related licenses designed for the same product. • Click a product to view the details of your licenses. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file.

Recovering licenses

Before recovering licenses, ensure that your device is connected to the internet.

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 **Recovery**.
   License Center automatically recovers all available licenses for applications installed on your devices.

Transferring a license to the new QNAP license server

This task only applies to existing licenses that have been activated using PAK.

Before transferring licenses, ensure the following.

- Your device 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 Manager** to review the license details.
6. Click **Close**.

Deleting a license

Before deleting a license, ensure that you have deactivated this 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.

15. Multimedia

QTS provides a range of applications and utilities for viewing, playing, and streaming multimedia files stored on the NAS.

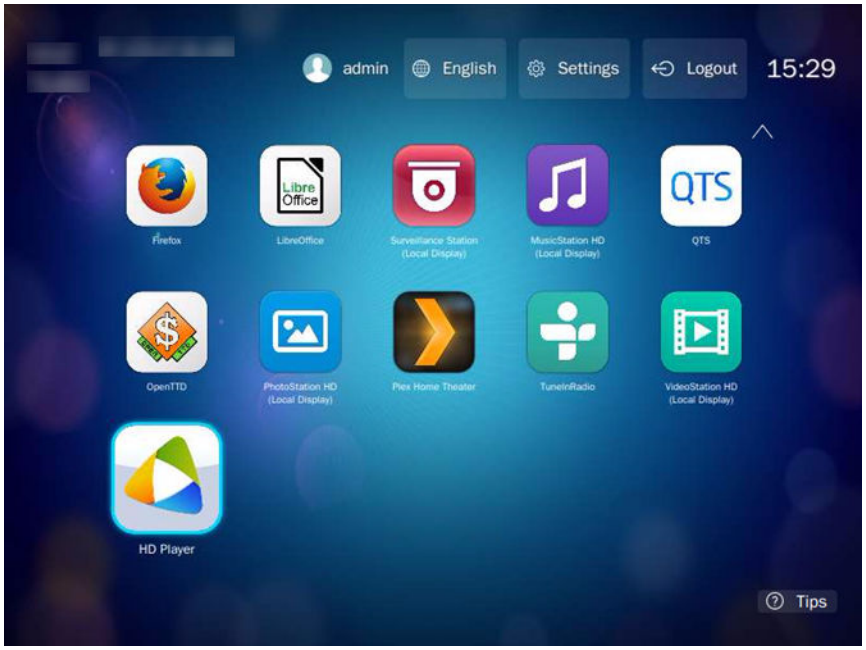
Application/Utility	Description
HybridDesk Station (HD Station)	Connect to an HDMI display to access multimedia content on your NAS.
DLNA Media Server	Configure your NAS as a Digital Living Network Alliance (DLNA) server to access media files on your NAS from devices on your home network.
Media Streaming Add-on	Stream media from your NAS to DLNA, Chromecast, and HDMI-connected devices.
Multimedia Console	Manage multimedia apps and content on the NAS. You can index files, transcode videos, and generate thumbnails for multimedia content.

HybridDesk Station (HD Station)

HybridDesk Station (HD Station) allows you to connect to an HDMI display and directly access multimedia content and use other applications on your NAS. You can use your NAS as a home theater, multimedia player, or desktop substitute. After installing HD Station and connecting the NAS to an HDMI display, you can navigate your NAS using HD Station.

HD Station requires:

- A TV or monitor with an HDMI port
- A mouse, keyboard, or remote control for navigation
- A graphics card (some NAS models only). Go to https://www.qnap.com to check the software specifications for your NAS and verify that it is compatible with HD Station.



Installing HD Station

1. Go to **Control Panel** > **Applications** > **HDMI Display Applications**.
2. Choose one of the following installation methods.

Installation Method	Steps
Guided installation	**a.** Click **Get Started Now**. The **HybridDesk Station** window appears. **b.** Review the list of selected applications. **Tip** All applications are selected by default. You can deselect applications that you do not want to install. **c.** Click **Apply**.
Manual installation	**a.** Under **Install Manually**, click **Browse**. **b.** Select HD Station. **c.** Click **Install**.

QTS installs HD Station and the selected applications.

Note

Multimedia Services must be enabled to play multimedia content in HD Station. Go to **Main Menu** > **Applications** > **Multimedia Console** to enable Multimedia Services.
HD Player, Photo Station, Music Station, and Video Station must also be installed on the NAS to play multimedia content from the respective applications.

Configuring HD Station

1. Go to **Control Panel** > **Applications** > **HDMI Display Applications** > **Local Display settings**.
2. Perform any of the following actions.

Action	Steps
Enable HD Station	Click **Enable**. **Note** HD Station must be disabled to perform this action.
Disable HD Station	Click **Disable**. **Note** HD Station must be enabled to perform this action.
Install all HD Station applications	**a.** Click **Install All Apps**. A dialog box appears. **b.** Click **OK**.
Update installed apps	Click **Update**.
Restart HD Station	Click **Restart**.
Remove HD Station and related applications	**a.** Click **Remove**. A dialog box appears. **b.** Click **OK**.

Action	Steps
Edit HD Station settings	**a.** Click **Settings**. The **Settings** window appears. **b.** Modify any of the following settings: • **Output resolution**: Change the resolution of HD Station. • **Overscan**: Reduce the visible area of a video displayed in HD Station. • **Enable Remote Desktop**: View the NAS HDMI output using your web browser. **Note** • Enabling Remote Desktop may affect the playback quality of local videos. • You must restart Remote Desktop after changing the output resolution. **Tip** You can also open and restart Remote Desktop from this screen.
Install HD Station apps	**a.** Under **Install Manually**, click **Browse**. **b.** Select the application. **c.** Click **Install**.

HD Station applications

Go to **App Center** > **HybridDesk Station** to install or configure applications used with HD Station.

Using HD Player in HD Station

You can use HD Player to browse and play multimedia content in Photo Station, Music Station, and Video Station.

1. Connect an HDMI display to the NAS.
2. Select your NAS account.
3. Specify your password.
4. Start HD Player.

5. Select your NAS account.
6. Specify your password.

HDMI local display and DLNA media server

You can stream multimedia content to High-Definition Multimedia Interface (HDMI) display applications or Digital Living Network Alliance (DLNA) devices. These services require you to enable Multimedia Services. To enable Multimedia Services, go to **Control Panel** > **Applications** > **Multimedia Console** > **Overview**.

Enabling HDMI display applications

1. Log in as administrator.
2. Go to **Control Panel** > **Applications** > **HDMI Display Applications**.
3. Locate the application you want to enable.
4. Optional: Configure the following settings.
   a. Click **Settings**.
   b. Configure the application settings.

      Note
      You may be required to update an application, connect a monitor, display to the NAS before successfully applying the settings.

   c. Click **Apply**.
5. Click **Enable**.
   A confirmation window appears.

   Note
   A confirmation window only appears if you have another application enabled.

6. Click **OK**.
   QTS enables the application.

Enabling and configuring DLNA media server

You can configure your NAS as a DLNA server, allowing you to access media files on your NAS through your home network using DLNA devices such as TVs, smartphones, and computers.

Important
You need to install Media Steaming Add-on from the App Center to enable and configure the DLNA Media Server. For details, see Media Streaming Add-on.

Media Streaming Add-on

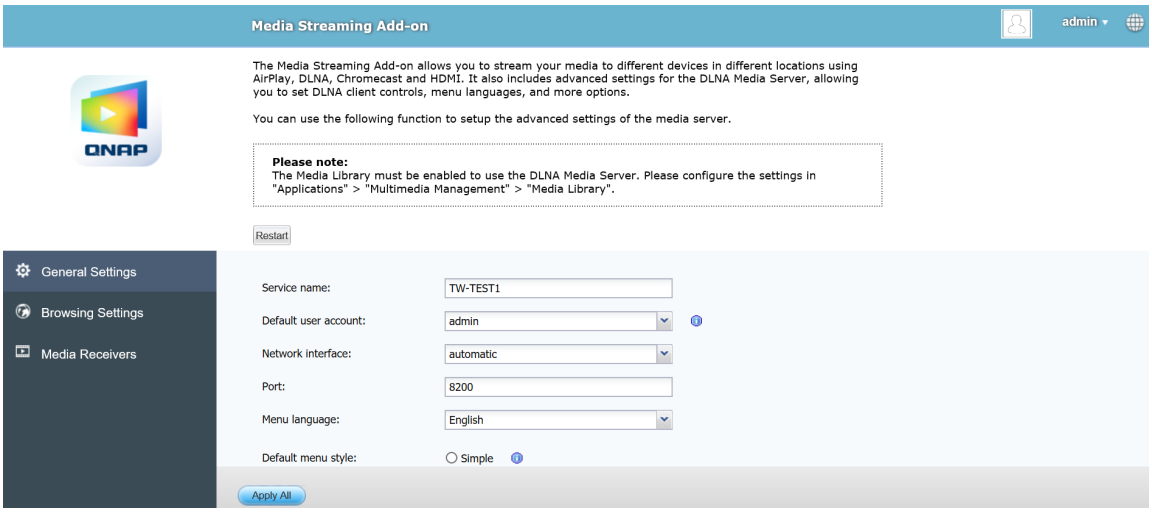
Media Streaming Add-on allows you to stream media from your NAS to different DLNA, Chromecast, and HDMI-connected devices simultaneously using the following QTS multimedia applications:

- File Station
- Photo Station
- Music Station
- Video Station

Go to App Center to install Media Streaming Add-on.

Tip

You can restart Media Streaming Add-on anytime by clicking **Restart** on the home screen.



Configuring general settings

1. Open **Media Streaming Add-on**.
   Media Streaming Add-on opens in a new tab.

   Note

   Media Streaming Add-on logs you in based on your QTS user credentials. If a login screen appears, you will need to specify your username and password to log in.

2. Go to **General Settings**.

3. Modify any of the following settings.

Setting	Description
Service name	This is the name that devices on the local network will see when connecting to the NAS.
Default user account	Select the user account that media devices receive content from. To connect using a different user account, you must specify the account's username and password in the connection settings of the media receiver.
Network interface	Select the network interface.
Port	Specify the port number.
Menu language	Select the language displayed for menu items.
Default menu style	Select the type of menu style. • **Simple** • **All categories** • **Custom** Select one of the **Custom** options and click **Customize** to configure the display options for the menu.
Always stream videos to Apple TV and Chromecast in original file formats	When selected, the NAS streams videos to these devices without transcoding or embedding subtitles. **Important** Ensure that Apple TV and Chromecast support the file formats of videos on your NAS when selecting this option.

4. Click **Apply All**.

Configuring browsing settings

1. Open **Media Streaming Add-on**.
   Media Streaming Add-on opens in a new tab.

   Note
   Media Streaming Add-on logs you in based on your QTS user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Browsing Settings**.

3. Modify any of the following settings.

Setting	Description
Display Photo	Select the display size of the thumbnail for photo albums.
Music title display style	Select the type of information that is displayed for music files.
Video title display style	Select whether video titles display the file name of the video or the embedded information.

4. Click **Apply All**.

Configuring media receivers

1. Open **Media Streaming Add-on**.
   Media Streaming Add-on opens in a new tab.

   Note
   Media Streaming Add-on logs you in based on your QTS user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Media Receivers**.
3. Perform any of the following actions.

Action	Steps
Enable device sharing	Select **Enable sharing for new media receivers automatically**. When enabled, newly discovered devices will automatically be allowed to connect to DLNA Media Server.
Scan for new devices	Click **Scan for devices** Media Streaming Add-on searches for new media devices connected to the NAS.
Modify device connections	Select or deselect media devices. Only selected devices can connect to DLNA Media Server.

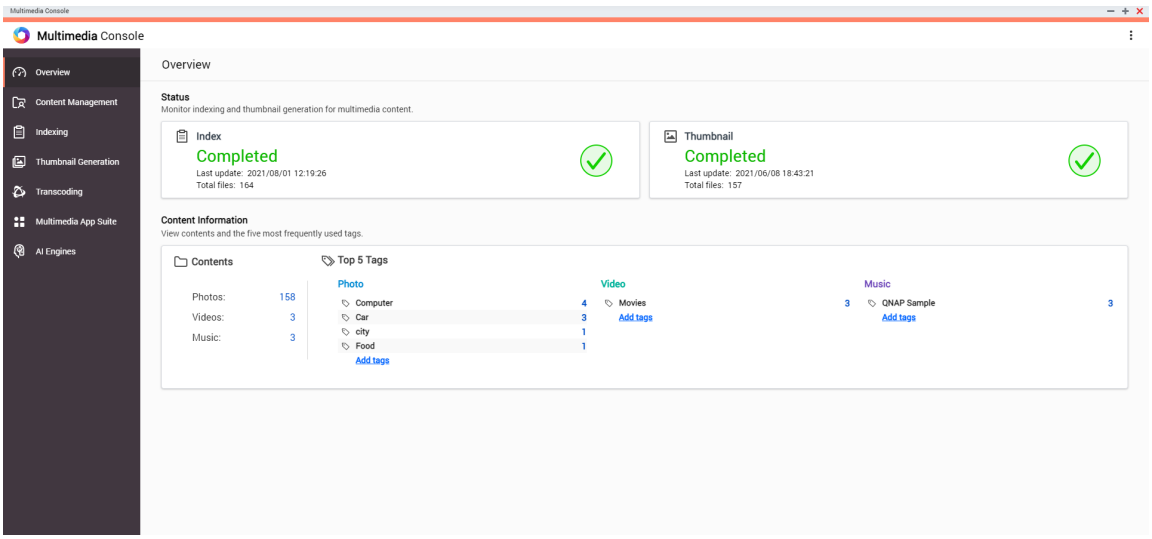
4. Click **Apply All**.

Multimedia Console

Multimedia Console helps you manage installed multimedia apps and content stored on the NAS. Multimedia Console can index files, transcode videos, and generate thumbnails for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Server.

Overview

The **Overview** screen displays the indexing and thumbnail generation status for multimedia files as well as the total number of photos, videos, and music files on your NAS



Editing content sources

The **Content Management** screen displays the content source folders for multimedia apps installed on the NAS. You can view and edit the content source folders for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Media Server.

1. Open Multimedia Console.
2. Go to **Content Management.**
3. Select an app or service.
4. Click **Edit**.
   The **Edit Content Sources** window appears.
5. Select or deselect content source folders.
   The **Selected Folder Paths** list updates.
6. Click **Apply**.

> **Tip**
> Click **Excluded System Sources** on the **Content Management** screen to view system folder paths that are excluded from Multimedia Services.

Indexing multimedia content

Multimedia Console improves content management, browsing, and playback when accessing files in various multimedia apps by scanning and indexing multimedia files on your NAS.

1. Open Multimedia Console.
2. Go to **Indexing**.
3. Select the **Priority**.
   - **Low (Default)**
   - **Normal**

   The **Priority** determines the amount of system resources allocated to the indexing process.
4. Select the type of **Text encoding**.
   The type of **Text encoding** determines the character encoding scheme that Multimedia Console uses to index text and data in your multimedia files. The default encoding scheme is Unicode.
5. Click **Apply**.

> **Tip**
> Click **Re-index** to rebuild the multimedia content database and revert dependent databases to their default settings.

Thumbnail generation

Multimedia Console generates thumbnails for multimedia files to improve browsing.

> **Note**
> - Thumbnail generation is enabled by default if Multimedia Services is enabled.
> - You can disable thumbnail generation in the upper right of the **Thumbnail Generation** screen.
> - Generating thumbnails may affect system performance.
> - Thumbnail generation for certain media file formats may require CAYIN MediaSign Player to be installed, and may also require a CAYIN MediaSign Player Plus license.

Managing thumbnails

1. Open Multimedia Console.
2. Go to **Thumbnail Generation** > **Status**.

3. Perform any of the following tasks.

Task	Steps
Pause thumbnail generation	**a.** Next to **Status**, click **Pause**. The **Pause** window opens. **b.** Select **Pause**. **c.** Click **OK**. **Tip** Click **Resume** when thumbnail generation is paused to resume thumbnail generation.
Postpone thumbnail generation	**a.** Next to **Status**, click **Pause**. The **Pause** window opens. **b.** Select **Postpone**. 1. Select the duration. **c.** Click **OK**. **Tip** Click **Resume** when thumbnail generation is postponed to resume thumbnail generation.
Remove thumbnails	**a.** Under **Used**, click **Remove All Thumbnails**. A dialog box appears. **b.** Click **OK**.
Regenerate thumbnails	**a.** Under **Used**, click **Regenerate All Thumbnails**. A dialog box appears. **b.** Click **OK**.

Configuring the thumbnail generation schedule

1. Open Multimedia Console.
2. Go to **Thumbnail Generation** > **Schedule**.

3. Next to **Schedule**, select one of the following options.

Option	Description
Generate in real time	Multimedia Console generates thumbnails as soon as new files are detected.
Generate using schedule	Multimedia Console generates thumbnails according to a specified schedule. **Note** When selected, you must specify a thumbnail generation schedule.
Generate manually	Multimedia Console generates thumbnails after clicking **Apply**.

4. Click **Apply**.

Configuring advanced settings

1. Open Multimedia Console.
2. Go to **Thumbnail Generation** > **Advanced Settings**.
3. Configure any of the following settings.

Setting	Description
Generation efficiency	Specifies the available system resource for thumbnail generation. Higher resource usage may impact performance. Available options are High, Medium, or Low.
Large thumbnails	When selected, Multimedia Console generates high-resolution thumbnails for media files.

Setting	Description
Image quality	Select **High** or **Low**. **Tip** • Click **See the difference** to view a side-by-side comparison of high- and low-quality thumbnails. • Click **Generate thumbnails using the original image when thumbnails are abnormal** to improve thumbnail generation accuracy.
Generation scope	Select **All multimedia files** or **Specific multimedia files**.
Excluded file sizes **Note** This option is only available when **Specific multimedia files** is selected for **Generation scope**.	Multimedia Console will not generate thumbnails for images that are smaller than the specified resolution.
Excluded file types **Note** This option is only available when **Specific multimedia files** is selected for **Generation scope**.	Multimedia Console will not generate thumbnails for the selected file types.

4. Click **Apply**.

Transcoding

The transcoding feature in Multimedia Console converts video files to MPEG-4 format for improved compatibility with media players on mobile devices, smart TVs, and web browsers. Transcoding can also scale down the resolution of video files to prevent buffering in slower network environments.

You can create and manage transcoding tasks and configure settings from the **Transcoding** screen in Multmedia Console.

Managing transcoding tasks

You can manage Background Transcoding and On-the-Fly Transcoding tasks from the Overview tab on the **Transcoding** screen.

Note

- Transcoding is only available for certain NAS models. Go to https://www.qnap.com/go/compatibility to view specifications for your NAS and verify that it is compatible.
- Transcoding uses additional NAS storage space to store transcoded files.

Type	Description
Background Transcoding	Background Transcoding converts videos asynchronously to minimize consumption of system resources if the video is accessed by multiple users simultaneously. The Background Transcoding tab displays the overall background transcoding status as well as additional information about specific background transcoding tasks. You can view and manage background transcoding tasks from this tab. You can manually add videos to background transcoding folders using File Station, Photo Station, or Video Station. For details on managing background transcoding folders, see Configuring background transcoding folders.
On-the-Fly Transcoding	On-the-Fly Transcoding converts videos in real time as you watch them. The On-the-Fly Transcoding tab displays information about on-the-fly transcoding tasks. You can view and manage on-the-fly transcoding tasks from this tab. **Note** • You cannot specify the output format for On-the-Fly Transcoding. • On-the-Fly Transcoding uses more system resources than Background Transcoding and may affect the performance of your NAS. **Tip** You can install CodexPack to increase transcoding speed and reduce system resource consumption. You can check whether your NAS supports GPU-acclerated transcoding on the **Transcoding Settings** screen. For details, see Configuring transcoding resources.

Configuring transcoding resources

1. Open Multimedia Console.
2. Go to **Transcoding** > **Settings** > **Transcoding Resources**.
3. Optional: Enable **GPU-accelerated transcoding**.
   a. Click **GPU Management**.
      The **System** > **Hardware** > **Graphics Card** screen appears.
   b. Configure graphics card settings.
4. Specify the **Maximum CPU usage** allocated to transcoding tasks.
5. Click **Apply**.

Configuring background transcoding settings

1. Open Multimedia Console.
2. Go to **Transcoding** > **Settings** > **Background Transcoding**.
3. Configure any of the following settings.

Setting	Description
Transcode manually-added videos first	Videos in File Station, Video Station, and Photo Station that are manually added will be transcoded first.
Embed subtitles when transcoding	Multimedia Console automatically embeds subtitles to videos when transcoding them.

4. Click **Apply**.

Configuring background transcoding folders

1. Open Multimedia Console.
2. Go to **Transcoding** > **Settings** > **Background Transcoding Folders**.

3. Perform any of the following tasks.

Task	User Action
Configure the scanning schedule for background transcoding folders	Select one of the following options: • **Scan in real time**: Multimedia Console scans background transcoding folders for new files and adds the files as background transcoding tasks as soon as they are detected. • **Scan using schedule**: Multimedia Console scans background transcoding folders for files according to a specified schedule. **Note** When selected, you must specify the time of day that Multimedia Console generates thumbnails. • **Scan manually**: Multimedia Console scans background transcoding folders only when you click **Scan Now**.
Add a background transcoding folder	**a.** Click **Add**. The **Add Background Transcoding Folders** window appears. **b.** Select a folder. **c.** Specify the output format. **d.** Click **Apply**.
Remove a background transcoding folder	**a.** Select a background transcoding folder. **b.** Click **Delete**.
Configure transcoding output format	**a.** Locate a background transcoding folder on the list. **b.** Select the output format. **Note** Multimedia Console upscales the video if the selected resolution is higher than the original resolution of the video. **c.** Click **Apply**.

Multimedia app suite

You can view statuses and configure user and group access permissions for installed multimedia apps and services from the **Multimedia App Suite** screen.

Configuring multimedia apps and services

1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.
3. Perform any of the following tasks.

Task	User Action
Install an app or service	**a.** Locate an app or service with the status **Not Installed** under the app or service name. **b.** Click **Not Installed**. The **App Center** and app installation windows open. **c.** Click + Install.
Enable an app or service	**a.** Locate an app or service with the status **Disabled** under the app or service name. **b.** Click **Disabled**. **c.** The app or service opens in a new window. **d.** Enable the app or service.
Disable an app or service	**a.** Locate an app or service with the status **Enabled** under the app or service name. **b.** Click **Enabled**. **c.** The app or service opens in a new window. **d.** Disable the app or service.

Configuring multimedia app permissions

1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.
3. Locate an app with access permissions.
4. Under **Permissions**, click the permission status.
The **Permission Settings** window opens.
5. Select a permission type.

Permission Type	Description
All Users	All users can access the app.

Permission Type	Description
Local Administrator Group Only	Only users in the local administrator group can access the app.
Custom	Specified users and user groups can access the app.

A dialog box appears.

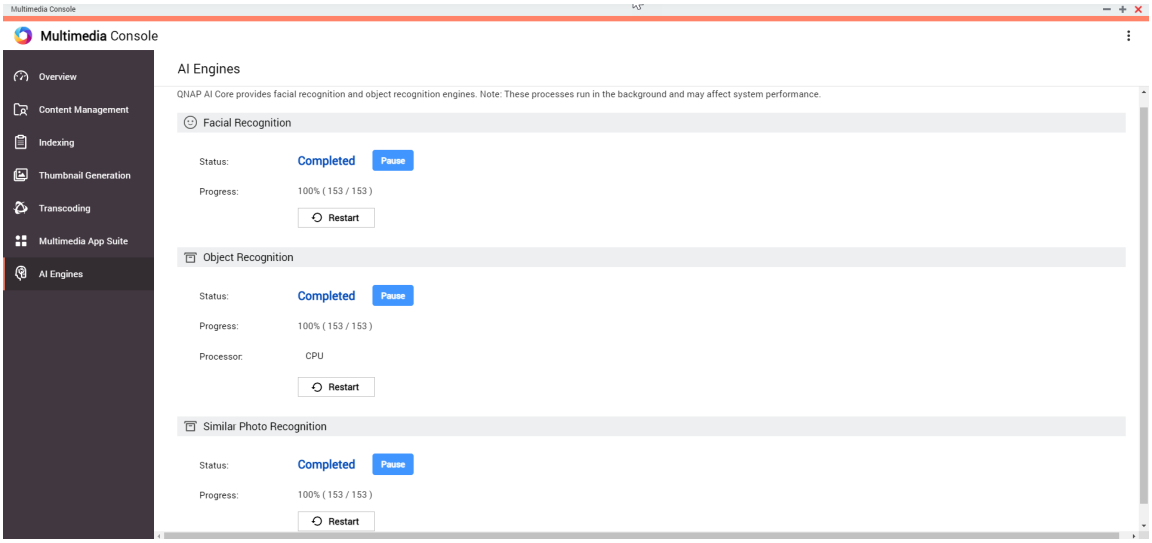
6. Click **OK**.
7. Perform any of the following actions.

Permission Type	User Action
All Users	Click **Close**.
Local Administrator Group Only	Click **Close**.

Permission Type	User Action
Custom	**a.** Select a user or user group type: • **Local** • **Domain** **b.** Choose to deny or allow access to selected users or groups. A dialog box appears. 1. Click **OK**. **c.** Filter the list by users or groups. **Tip** Use the **Search** field to quickly find users or groups. **d.** Select a user or group. **e.** Click **Add**. The user or group is added to the Selected Users/Groups list. **Tip** • Select a user or group and click **Delete** to remove the user or group from the list. • Click **Delete All** to remove all users or groups from the list. **f.** Click **Save**. **g.** Click **Close**.

Installing and managing AI engines

QNAP AI Core provides facial and object recognition engines.



1. Install QNAP AI Core.
   For details, see Installing an app from App Center.

   Note
   This process can take a while.

2. Open Multimedia Console.
3. Select **AI Engines**.

   Tip

   - QNAP AI Core supports Google TPU devices. To check if the Google TPU device is successfully running on the NAS, go to **Control Panel** > **System** > **Hardware** > **Hardware Resources**.
   - You can check the status of the Google TPU device on the top right corner of the screen. If QNAP AI Core is running the Google TPU device, the status changes to **Google TPU: Running**. If the Google TPU device is not running, the status changes to **Google TPU: Stopped**.

4. Locate an AI engine you want to manage and select one of the following options.

Option	User Action
Pause	**a.** Click **Pause**. The **Pause** window opens. **b.** Select one of the following options. • **Pause**: Pauses the engine now. • **Postpone**: Pauses the engine after a specific time period. **Note** You can postpone by 1, 2, or 5 hours. **c.** Click **OK**.
Restart	**a.** Click **Restart**. A confirmation message appears. **b.** Click **OK**.

QNAP AI Core pauses or restarts the AI engine.

16. QuLog Center

QuLog Center allows you to centrally manage and monitor logs from local devices and remote devices. You can specify log filters, create notification rules, and configure log settings to stay informed of your device status and important events. You can view and manage system logs in **Control Panel** > **System** > **QuLog Center**. For details about QuLog Center concepts and terms, see the following table.

Terms	Definition
Event Log	The event log is a record of system events, such as system, security, and application notifications. Events are stored by the device operating system for administrators to diagnose system problems and troubleshoot issues.
Access Log	The access log is a detailed record of user access to applications and files on a device.
Local Device	The current device you are logged in.
QuLog Service	The QuLog Service is a remote log management service that allows you to centrally manage remote system logs on the local device. The QuLog Service also allows you to send local device logs to a remote QuLog Center or to a Syslog Server.
Log Receiver	The local device that is the recipient of all remote device logs. The Log Receiver functions as the central log management platform for up to 500 remote devices.
Log Sender	A local device that sends logs to a remote QuLog Center on another device or to a Syslog Server.
Sender Device	A remote device that sends logs to the local Log Receiver.

Monitoring logs

The **Overview** screen provides statistical graphics to help you visualize log data and monitor device status.

Event log

The **Overview** > **Event Log** tab provides the following widgets to visualize the statistical data of the event logs from your devices.

Important
You must configure a log destination to enable the event log feature. For details, see Configuring Event Log Settings.

Tip

The **Overview** > **Event Log** page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Widget	Description
Logs Over Time	This widget displays a line chart to visualize the number of log entries over the specified period of time. **Tip** • Click ··· to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time.
Top 5 Service Error Logs	This widget displays the five services that have the largest numbers of error log entries.
Top 5 Service Warning Logs	This widget displays the five services that have the largest numbers of warning log entries.

Access logs

The **Overview** > **Access Log** tab provides the following widgets to visualize the statistical data of the access logs from your devices.

Tip

The **Overview** > **Access Log** page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Section	Description
Logs Over Time	This widget displays a line chart to visualize the number of log entries over the specified period of time. **Tip** • Click ··· to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time.
Currently Online	This widget lists the current online users and provides the information of their user sessions.
Connection Types	This widget displays a pie chart to visualize the numbers of user sessions for each communication protocol.
Logged in	This widget displays a pie chart to visualize the numbers of successful login attempts using each IP address or user account.
Failed to log in	This widget displays a pie chart to visualize the numbers of failed login attempts using each IP address or user account.

Local device logs

The **Local Device** screens allow you to monitor event logs, access logs, and online user status on one local device. You can also configure log filters, log settings, and remove event indicators.

Local event logs

You can monitor and manage event logs from local devices in **Local Device** > **Event Log**.

Important

- You must configure a log destination to enable the local event log feature.
  For details, see Configuring event log settings.
- QuLog Center can download or export a maximum of 10,000 log entries. You can use log filters to specify the maximum number of log entries per file for download or export.
  For details, see Adding a Log Filter.
- QuLog Center can store up to 5,000,000 event log entries but can only query and process up to 100,000 log entries at a time. By default, the most recent logs are displayed first. You can perform a search to locate earlier logs.

On the **Local Device** > **Event Log** screen, you can perform the following tasks:

Task	Steps
Select a group mode	**1.** Click . **2.** Select one of the following grouping modes. • **No grouping**: this mode displays and lists all log entries. • **By app**: this mode groups log entries by app name. • **By date**: this mode groups log entries by date. • **By content**: this mode groups log entries by log content. • **By user**: this mode groups log entries by users. • **By source IP**: this mode groups log entries by source IP address.
Select a display style	**1.** Click . **2.** Select a display style. **Tip** You can also click **Add Style** to create a display style. For details, see Configuring a Display Style.
Export logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Export**. **3.** Select an export file format. QuLog Center supports CSV and HTML log file formats. **4.** Optional: Compress the export file and specify a password. **5.** Specify the destination shared folder for exporting logs. **a.** Click **Browse**. The **Select a shared folder** window appears. **b.** Select a shared folder. **6.** Click **Export**.

Task	Steps
Download export logs	1. Click . The **Export Logs** drop-down menu appears. 2. Click **Download**. 3. Select an export file format. QuLog Center supports CSV and HTML log file formats. 4. Optional: Compress the export file and specify a password. 5. Click **Download**. The log file is downloaded to your computer.
Perform a search	1. Specify keywords in the search field. **Tip** For advanced search options, click . 2. Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a custom filter tab for local event logs.
Select display items	1. Click . 2. Select the item category to display.
Create an event notification rule	You can quickly create an event notification rule using a log entry. This allows you to receive notifications for events similar to the selected log entry. 1. Locate a log entry. 2. Click . 3. Select **Create event notification rule**. Notification Center opens and the **Create event notification rule** windows appears. For details on creating and managing notification rules, see Notification Center.

Task	Steps
Create an event flag rule	**1.** Locate a log entry. **2.** Click ⋮. **3.** Select **Create Event Flag Rule**. The **Create Event Flag Rule** window appears. **4.** Click **Create**. The event is flagged. Go to **Log Settings** > **Event Indicators** to view all event flags.
Select all log entries	**1.** Select one or more log entries. **2.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **3.** Click **Select all**.
Invert selection	**1.** Select one or more log entries. **2.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **3.** Click **Invert selection**.
Copy one or more log entries	**1.** Select one or more log entries. **2.** Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	**1.** Select one or more log entries. **2.** Click . A confirmation message appears. **3.** Click **Yes**.

Local access logs

You can monitor and manage access logs from local devices in **Local Device** > **Access Log**.

Important

- You must configure a log destination to enable the access logs feature.
  For details, see Configuring access log settings.
- QuLog Center can download or export a maximum of 10,000 log entries. You can use log filters to specify the maximum number of log entries per file for download or export.
  For details, see Adding a Log Filter.
- QuLog Center can to store up to 5,000,000 access log entries but can only query and process up to 100,000 log entries at a time. By default, the most recent logs are displayed first. You can perform a search to locate earlier logs.

On the **Local Device** > **Access Log**screen, you can perform the following tasks:

Task	Steps
Select a group mode	**1.** Click . **2.** Select one of the following grouping modes. • **No grouping**: this mode displays and lists all log entries. • **By date**: this mode groups log entries by date. • **By user**: this mode groups log entries by user. • **By source IP**: this mode groups log entries by source IP address.
Select a display style	**1.** Click . **2.** Select a display style. **Tip** You can also click **Add Style** to create a display style. For details, see Configuring a Display Style.

Task	Steps
Export logs	1. Click . The **Export Logs** drop-down menu appears. 2. Click **Export**. 3. Select an export file format. QuLog Center supports CSV and HTML log file formats. 4. Optional: Compress the export file and specify a password. 5. Specify the destination shared folder for exporting logs. a. Click **Browse**. The **Select a shared folder** window appears. b. Select a shared folder. 6. Click **Export**.
Download export logs	1. Click . The **Export Logs** drop-down menu appears. 2. Click **Download**. 3. Select an export file format. QuLog Center supports CSV and HTML log file formats. 4. Optional: Compress the export file and specify a password. 5. Click **Download**. The log file is downloaded to your computer.
Perform a search	1. Specify keywords in the search field. 2. Press **Enter**. 3. Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a custom filter tab for local access logs.
Select display items	1. Click . 2. Select the item category to display.

Task	Steps
Select all log entries	**1.** Select one log entry. **2.** Click **Select multiple entries**. The **Select multiple entries** drop-down menu appears. **3.** Click **Select all** . All log entries are selected.
Invert selection	**1.** Select one log entry. **2.** Click **Select multiple entries**. The **Select multiple entries** drop-down menu appears. **3.** Click **Invert selection**.
Copy one or more log entries	**1.** Select one or more log entries. **2.** Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	**1.** Select one or more log entries. **2.** Click . A confirmation message appears. **3.** Click **Yes**.
Add one or more log entry to the block list	**1.** Select one or more log entries. **2.** Click **Add to block list**. The **Add to block list** drop-down menu appears. **3.** Select a block period option.

Online users

From the **Local Device** > **Online Users** screen, you can find a list of online users and related information such as login date and time, username, source IP address, computer name, connection type, accessed resources, and total connection time.

You can perform the following tasks:

Tasks	Steps
Remove a connection	1. Locate a user from the list. 2. Right-click the user. 3. Select **Disconnect**. A confirmation message appears. 4. Click **Yes**.
Block a user	1. Locate a user from the list. 2. Right-click the user. 3. Select **Add to block list**. 4. Select a block period option.
Remove the connection and block the user	1. Locate a user from the list. 2. Right-click the user. 3. Select **Disconnect and add to a block list**. A confirmation message appears. 4. Select a block period option.
Control the visible columns	1. Click +. 2. Select the item category to display.

Creating a custom filter tab for local device logs

You can create custom filter tabs for local event logs and local access logs. The customized filter tabs can filter logs or user information based on specified keywords or criteria. For details, see the following topics:

- Creating a custom filter tab for local event logs
- Creating a custom filter tab for local access logs

Creating a custom filter tab for local event logs

1. Open QuLog Center.
2. Go to **Local Device** > **Event Log**.
3. Go to the search bar.
4. Click ▾.
   The **Advanced Search** window appears.

5. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click ▾. The severity level drop-down menu appears. **b.** Select a severity level option.
Service	**a.** Click ▾. The service drop-down menu appears. **b.** Select a service. The **Category** option appears. **Note** The **Category** option only appears when you specify the service. **c.** Specify the service **Category**.
Date	**a.** Click ▾. The date drop-down menu appears. **b.** Select a date option.
Content	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the content keywords.
User	**a.** Click ▾. The user condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.

Fields	Steps
Client App	**a.** Click ▾. The client app condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Flag	**a.** Click ▾. The flag condition option appears. **b.** Select a condition. **c.** Specify the keywords.

6. Optional: Click **Reset** to clear all search filters.
   Respecify search filters as many times as required.
7. Click **Search**.
   The list of filtered results is displayed.
8. Click **Add as Customized Tab**.
   The **Add as Customized Tab** window appears.
9. Enter a tab name.
10. Click **Apply**.
    - The custom filter tab is created.
    - The custom filter tab is displayed next to the **Main** tab.

Creating a custom filter tab for local access logs

1. Open QuLog Center.
2. Go to **Local Device** > **Access Log**.
3. Go to the search bar.
4. Click ▾.
   The **Advanced Search** window appears.

5. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click ▾. The severity level drop-down menu appears. **b.** Select a severity level option.
Accessed Resources	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Date	**a.** Click ▾. The date drop-down menu appears. **b.** Select a date option.
Connection type	**a.** Click ▾. The connection type option appears. **b.** Select a connection type.
User	**a.** Click ▾. The user condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Action	**a.** Click ▾. The action drop-down menu appears. **b.** Select an action option.
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.

Fields	Steps
Client App	**a.** Click ▾. The client app condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Computer Name	**a.** Click ▾. The computer name condition option appears. **b.** Select a condition. **c.** Specify the keywords.

6. Optional: Click **Reset** to clear all search filters.
   Respecify search filters as many times as required.
7. Click **Search**.
   The list of filtered results is displayed.
8. Click **Add as Customized Tab**.
   The **Add as Customized Tab** window appears.
9. Enter a tab name.
10. Click **Apply**.
    - The custom filter tab is created.
    - The custom filter tab is displayed next to the **Main** tab.

Local log settings

Log Settings allows you to configure the following types of settings: event logs, access logs, display styles, and event indicators.

Configuring event log settings

You can specify the database size and the log language or delete all the log entries for event logs.

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Event Log Settings**.

3. Specify the following settings:

Settings	Steps
Destination **Important** • You must configure a log destination to enable event logging features. • You cannot select a volume that is encrypted or has less than 10% of free volume space.	**a.** Click ▾. The log destination option drop-down menu appears. **b.** Select a log destination.
Maximum number of entries	**a.** Click ▾. The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed. The log database size is specified.
Log retention time	**a.** Click ▾. The log retention time drop-down menu appears. **b.** Select the log retention time.
Archive overflow log entries to a standby log destination	**a.** Click **Archive and move log entries to the specified location after reaching the database limit**. The destination folder option is activated. **b.** Click **Browse**. The **Select a shared folder** window appears. **c.** Select a shared folder. **d.** Click **OK**. The shared folder is selected as the standby log destination.

4. Optional: Delete all event logs.
   a. Click **Delete All Event Logs**.
   A confirmation message appears.

b. Click **Yes**.

> **Warning**
> You cannot restore deleted logs.

5. Select the log language.

   a. Click ▾.
   The log language drop-down menu appears.

   b. Select a language.

6. Click **Apply**.

Configuring access log settings

You can specify the database size, log retention time, connection type, or delete all access log entries.

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Access Log Settings**.
3. Specify the following settings:

Settings	Steps
Destination **Important** • You must configure a log destination to enable event logging features. • You cannot select a volume that is encrypted or has less than 10% of free volume space.	a. Click ▾. The log destination option drop-down menu appears. b. Select a log destination.
Maximum number of entries	a. Click ▾. The maximum number of entries option drop-down menu appears. b. Select the maximum number of entries allowed.

Settings	Steps
Log retention time	**a.** Click ▾. The log retention time drop-down menu appears. **b.** Select the log retention time.
Connection Types	Select the connection types you want to log. **Tip** You can select multiple connection types.

4. Optional: Delete all access logs.
   a. Click **Delete All Access Logs**.
   A confirmation message appears.
   b. Click **Yes**.

   Warning
   You cannot restore deleted logs.
5. Click **Apply**.

Configuring a display style

You can customize your log display style to enhance readability or to highlight certain entries.

1. Open QuLog Center.
2. Open **Display Settings** through one of the following methods:

Log type	Steps
Event Log	Go to **Local Device** > **Event Log** > **Display style**.
Access Log	Go to **Local Device** > **Access Log** > **Display style**.

3. Click ▾.
   The display style drop-down menu appears.
4. Click **Settings**.
   The **Display Style Settings** window appears.

5. Perform one or more of the following tasks:

Task	Steps
Add a display style	**a.** Click **Add Style**. The **Add Style** window appears. **b.** Specify a name for the style. **c.** Click **Apply**.
Delete a style	**a.** Select a display style. **b.** Click **Delete Style**. A confirmation message appears. **c.** Click **Yes**.
Add a rule to a display style	**a.** Select a display style. **b.** Click **Add Rule**. The **Style Rule** window appears. **c.** Select a field. **d.** Select a keyword. **e.** Select one or more formatting effects. **Tip** You can instantly preview the results of the selected formatting effects. **f.** Click **Apply**.

Task	Steps
Edit a rule	**a.** Select a display style. **b.** Select a rule from the list. **c.** Click **Edit**. The **Style Rule** window appears. **d.** Select a field. **e.** Specify the condition. **f.** Select one or more formatting effects. **Tip** You can instantly preview the results of selected formatting effects. **g.** Click **Apply**.
Remove a rule	**a.** Select a display style. **b.** Select a rule from the list. **c.** Click **Delete**. A confirmation message appears. **d.** Click **Yes**.
Specify the priority of rules	**a.** Select a display style. **b.** Select a rule from the list. **c.** Beside **Priority**, click ^ or v to change its priority. **Note** The formatting results of rules with a higher priority overwrite those with a lower priority.

Removing event indicators

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Event Indicators**.

3. Select an event flag rule.

   Tip
   Click the box in the top left column to select all event flag rules.

4. Click **Remove** or .

The event flag rule is removed.

QuLog Service

QuLog Service allows you to centrally manage logs from multiple remote devices. You can configure a single device as a Log Receiver to manage and monitor all incoming system logs from other devices, or configure the device as a Log Sender that sends all system logs to a remote QuLog Center.

Configuring log sender settings

The Log Sender allows you to send event logs and access logs on the local device to a remote QuLog Center or Syslog Server.

Adding a destination IP address

1. Open QuLog Center.
2. Select one of the following options:

Options	User Actions
Send to QuLog Center	**a.** Go to **QuLog Service** > **Log Sender** > **Send to QuLog Center**. **b.** Enable **Send logs to a remote QuLog Center**. Event logs and access logs from the local device are sent to a remote QuLog Center.
Send to Syslog Server	**a.** Go to **QuLog Service** > **Log Sender** > **Send to Syslog Server**. **b.** Enable **Send logs to a remote syslog server**. Event logs and access logs from the local device are sent to a remote syslog server.

3. Click **Add Destination**.
   The **Add Destination** window appears.
4. Specify the following IP address information:
   - **Hostname/IP Address**

> **Tip**
> You can enter the destination IP address manually or click **Search** to automatically select a device from your local network. This option is only available for sending logs to a remote QuLog Center.

- **Port**
- **Transfer protocol**
- **Log type**
- **Format**

> **Note**
> You can click **Send a Test Message** to test the connection. This option is only available for sending logs to a remote QuLog Center.

5. Click **Apply**.

Editing a destination IP address

1. Open QuLog Center.
2. Go to **Log Sender**.
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select a destination IP address.
5. Click .
   The **Edit Destination** window appears.
6. Edit the IP address information.
   For details, see Adding a Destination IP Address.
7. Click **Apply**.

Sending a test message

1. Open QuLog Center.
2. Select one of the following options:

Methods	Actions
Add Destination IP Address	Add a destination IP address. For details, see Adding a destination IP address
Send a Test Message	**a.** Select a destination IP address. **b.** Click **Send a Test Message**.

Methods	Actions
	Click  .

A test message is sent to the destination IP address to test the network connection.

Removing a destination IP address

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Sender**.
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select one or more destination IP addresses.
5. Click **Remove** or  .
   A confirmation message window appears.
6. Click **Yes**.
   The destination IP address is removed.

Configuring log reciever settings

The Log Reciever allows you to configure a local device as the recipient of remote device logs. You can centrally manage and monitor event logs and access logs from remote QNAP devices. Additionally, you can configure customized filters to search for logs efficiently.

Configuring log receiver general settings

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **General Settings**.
3. Select **Receive logs from a remote QuLog Center**.
4. Select transfer protocols and then specify the port number.

   Note
   QuLog Center supports TCP and UDP protocols.
5. Optional: Click **Enable Transport Layer Security (TLS)**.
6. Select **Event Log** or **Access Log**.

7. Specify the following settings:

Settings	Steps
Destination	**a.** Click ▾. The log destination option drop-down menu appears. **b.** Select a log destination. **Important** You cannot select a volume that is encrypted or has less than 10% of free volume space.
Maximum number of entries	**a.** Click ▾. The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed. The log database size is specified.
Log retention time	**a.** Click ▾. The log retention time drop-down menu appears. **b.** Select the log retention time.
Archive overflow log entries to a standby log destination	**a.** Click **Archive and move log entries to the specified location after reaching the database limit**. The destination folder option is activated. **b.** Click **Browse**. The **Select a shared folder** window appears. **c.** Select a shared folder. **d.** Click **OK**. The shared folder is selected as the standby log destination.
Delete all event logs	**a.** Click **Delete All Event Logs**. A confirmation window appears. **Warning** You cannot restore deleted logs. **b.** Click **Yes**.

8. Click **Apply**.

Log filter configurations

You can specify log filter conditions for system logs received from multiple sender devices on the Log Receiver to simplify locating specific types of logs and monitoring large volume of logs.

Configuring a log filter criterion

You can specify log filter criteria to choose the types of log entries that will be received by Log Receiver.

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Filter Criteria**.
3. Select **Event Log** or **Access Log**.
4. Click **Add Filter Criteria**.
   The filter criteria window appears.
5. For event logs, specify one or more of the following settings: **Severity level**, **User**, **Source IP**, **Service**, **Category**, **Content**, **Hostname**.
6. For access logs, specify one or more of the following settings: **Severity level**, **User**, **Source IP**, **Accessed resources**, **Hostname**, **Connection type**, **Action**.
7. Click **Apply**.

QuLog Center adds the specified log filter criteria.

Editing a log filter criterion

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Filter Criteria**.
3. Go to **Event Log** or **Access Log**.
4. Select a filter criteria.
5. Optional: Click **Reset** to clear all filter criteria settings.
6. Click .
   The **Filter Criteria** window appears.
7. Edit the log filter fields.
   For details, see Configuring a Log Filter Criterion.
8. Click **Apply**.
   All changes are applied.

Deleting a log filter criterion

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Filter Criteria**.

3. Select **Event Log** or **Access Log**.
4. Select a filter criteria.
5. Click .
   A confirmation window appears.
6. Click **Yes**.

Importing a custom filter criterion

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Filter Criteria**.
3. Click **Event Log** or **Access Log**.
4. Click **Add Filter Criteria**.
5. Go to **Import custom filter criteria from the selected tab**.
6. Click .
   The custom filter criteria drop-down menu appears.
7. Select the custom filter tab from the drop-down menu.

   Note
   For details on how to create a custom filter tab, see the following topics:
   - Creating a custom filter tab for event logs on a sender device
   - Creating a custom filter tab for access logs on a sender device

   The selected custom filter criteria are applied to the log.

Viewing and managing remote logs

You can view and manage remote logs under the Sender Devices section in QuLog Center. This section lists all remote devices that send their logs to the QuLog Center on the local device. You can monitor logs from all sender devices or from individual sender devices. QuLog Center can manage up to 500 sender devices on a log receiver.

Managing event logs on the log receiver

You can monitor and manage event logs received by the **Log Reciever** in **QuLog Service** > **All Devices** > **Event Log**. You can also monitor event logs from individual sender devices.

Important
You must configure the log destination of the log receiver to enable this feature. For details, see Configuring Log Receiver General Settings.

On the **Event Log** tab, you can perform the following tasks:

Task	Steps
Select a group mode	1. Click . 2. Select one of the following grouping modes. • **No grouping**: this mode displays and lists all log entries. • **By app**: this mode groups log entries by app name. • **By date**: this mode groups log entries by date. • **By content**: this mode groups log entries by log content. • **By user**: this mode groups log entries by users. • **By source IP**: this mode groups log entries by source IP address. • **By Host Name**: this mode groups log entries by the host name.
Select a display style	1. Click . 2. Select a display style. **Tip** You can also click **Add Style** to create a display style. For details, see Configuring a Display Style.
Create an event flag rule	You can quickly create an event flag rule using a log entry. This allows you to set event indicators for malware detection. 1. Locate a log entry. 2. Click . 3. Select **Create event flag rule**. The **Create Event Flag Rule** window appears. 4. Click **Create**. The log flag rule is created.

Task	Steps
Export logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Export**. **3.** Select an export file format. QuLog Center supports CSV and HTML log file formats. **4.** Select the maximum number of log entries per file. **5.** Optional: Compress the export file and specify a password. **6.** Specify the destination shared folder for exporting logs. **a.** Click **Browse**. The **Select a shared folder** window appears. **b.** Select a shared folder. **7.** Click **Export**.
Download export logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Download**. **3.** Select an export file format. QuLog Center supports CSV and HTML log file formats. **4.** Optional: Compress the export file and specify a password. **5.** Click **Download**. The log file is downloaded to your computer.
Perform a search	**1.** Specify keywords in the search field. **2.** Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a custom filter tab for event logs on a sender device.
Select display items	**1.** Click . **2.** Select the items to display.

Task	Steps
Select all log entries	1. Select one or more log entries. 2. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 3. Click **Select all**.
Invert selection	1. Select one or more log entries. 2. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 3. Click **Invert selection**.
Copy one or more log entries	1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click **Yes**.

Managing access logs on the log receiver

You can monitor and manage access logs received by the **Log Receiver** in **QuLog Service** > **All Devices** > **Access Log**. You can also monitor access logs from individual sender devices by clicking on the device.

Important
You must configure the log destination of the log receiver to enable this feature. For details, see Configuring Log Receiver General Settings.

On the **Access Log** tab, you can perform the following tasks:

Task	Steps
Select a group mode	**1.** Click . **2.** Select one of the following grouping modes. • **No grouping**: this mode displays and lists all log entries. • **By date**: this mode groups log entries by date. • **By user**: this mode groups log entries by user. • **By source IP**: this mode groups log entries by source IP. • **By Host Name**: this mode groups log entries by host name.
Select a display style	**1.** Click . **2.** Select a display style. **Tip** You can also click and select **Create a Style** to create a display style. For details, see Configuring a Display Style.
Export logs	**1.** Click . The **Export Logs** window appears. **2.** Select an export file format. **3.** Optional: Compress the export file and specify a password. **4.** Click **Export**.
Download exported logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Download**. **3.** Select an export file format. QuLog Center supports CSV and HTML log file formats. **4.** Optional: Compress the export file and specify a password. **5.** Click **Download**. The log file is downloaded to your computer.

Task	Steps
Perform a search	1. Specify keywords in the search field. 2. Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a custom filter tab for access logs on a sender device.
Select display items	1. Click +. 2. Select the items to display.
Select all log entries	1. Select one or more log entries. 2. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 3. Click **Select all**.
Invert selection	1. Select one or more log entries. 2. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 3. Click **Invert selection**.
Copy one or more log entries	1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click **Yes**.

Logging in a sender device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices**.
3. Select a device.
4. Click **Settings**.

5. Specify the following:
   - **Host IP address**
   - **Port**
   - **Username**
   - **Password**
6. Optional: Select **Secure login (HTTPS)**.
7. Click **Sign in**.
   - You are logged into the sender device.
   - All destination IP addresses of the sender device are listed.
   - You can configure the destination for sender device logs.
     For details, see Configuring log sender settings.

Creating a custom filter tab for event logs on a sender device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices**.
3. Click on a sender device.
4. Go to **Event Log** .
5. Go to the search bar.
6. Click .
7. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click . The severity level drop-down menu appears. **b.** Select a severity level option.

Fields	Steps
Service	**a.** Click ▾. The service drop-down menu appears. **b.** Select an service. The **Category** option appears. **Note** The **Category** option does not appear if you select any services or do not specify the application. **c.** Specify the service **Category**.
Date	**a.** Click ▾. The date drop-down menu appears. **b.** Select a date option.
Content	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the content keywords.
User	**a.** Click ▾. The user condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.
Hostname	**a.** Click ▾. The hostname condition option appears. **b.** Select a condition. **c.** Specify the keywords.

Fields	Steps
Client App	**a.** Click ▾. The client app condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Flag	**a.** Click ▾. The flag condition option appears. **b.** Select a condition. **c.** Specify the keywords.

8. Optional: Click **Reset** to clear all search filters.
   Respecify search filters as many times as required.
9. Click **Search**.
   The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
    The **Add as Customized Tab** window appears.
11. Enter a tab name.
12. Click **Apply**.
    - The custom filter tab is created.
    - The custom filter tab is displayed next to the **Main** tab.

Creating a custom filter tab for access logs on a sender device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices**.
3. Click on a sender device.
4. Go to **Access Log** .
5. Go to the search bar.
6. Click ▾.

7. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click ▾. The severity level drop-down menu appears. **b.** Select a severity level option.
Accessed Resources	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Date	**a.** Click ▾. The date drop-down menu appears. **b.** Select a date option.
Connection type	**a.** Click ▾. The connection type option appears. **b.** Select a connection type.
User	**a.** Click ▾. The user condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Action	**a.** Click ▾. The action drop-down menu appears. **b.** Select an action option.
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.

Fields	Steps
Hostname	**a.** Click ▾. The hostname condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Client App	**a.** Click ▾. The client app condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Computer Name	**a.** Click ▾. The computer name condition option appears. **b.** Select a condition. **c.** Specify the keywords.

8. Optional: Click **Reset** to clear all search filters.
   Respecify search filters as many times as required.
9. Click **Search**.
   The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
    The **Add as Customized Tab** window appears.
11. Enter a tab name.
12. Click **Apply**.
    - The custom filter tab is created.
    - The custom filter tab is displayed next to the **Main** tab.

Configuring event indicators on the sender device

The event severity indicators on the device list are displayed according to the event severity level (information, warning, and error) that occurs over a specified period. Only the highest severity level icon is displayed when multiple events occur.

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices**.
3. Select a device.
4. Got to the **Event Indicators** tab.

5. Click ▾.
   The event period drop-down menu appears.
6. Select the event period.
   Events that meet the specified criteria are listed in the Event Flag Rules table below.

   Tip
   You can remove event flag rules from the list.

Notification settings

You can configure notification rules in Notification Center. You can also create filters for sending local NAS access logs, QuLog Service event logs, and QuLog Service access logs.

Configuring notification rule settings

QuLog Center can send notifications to recipients when the **Log Receiver** receives event logs or access logs from the **Log Sender**.

1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select the log types.
4. You can perform any of the following actions:

Setting	Steps
Create a notification rule **Important** You must select the **Transfer status** option in **System Notification Rules** when creating QuLog Center notification rules for receiving local device logs, QuLog Service event logs, and QuLog Service access logs. To enable the **Transfer status** option, go to **Notification Center** > **System Notification Rules** > **QuLog Center** > **Transfer status**.	a. Click **Configure Notification Rule**. Notification Center opens. Follow the instructions on the **Create event notification rule** wizard to add an event notification rule for QuLog Center. For details, see Creating an Event Notification Rule.
Edit a notification rule	Click ✎.
Enable or disable a notification rule	Click toggle.

Setting	Steps
Delete a notification rule	**a.** Click . A confirmation message window appears. **b.** Click **Yes**. The notification rule is deleted.
View notification history	Click **View notification history**. Notification Center opens and displays the QuLog Center notification history page.

Adding a log filter

You can add filter criteria to local NAS access logs, QuLog Service event logs, and QuLog Service access logs. The filtered log results are sent to Notification Center.

1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select a system log type.
4. Click **Add Filter Criteria**.
   The filter criteria window appears.
5. For event logs, specify one or more of the following settings: **Severity level**, **User**, **Source IP**, **Service**, **Category**, **Content**, **Hostname**.
6. For access logs, specify one or more of the following settings: **Severity level**, **User**, **Source IP**, **Accessed resources**, **Hostname** (available on QuLog Service devices only), **Connection type**, **Action**.
7. Click **Apply**.
   The filter is applied to logs sent to Notification Center.

Editing a log filter

1. Open QuLog Center.
2. Go to **QuLog Service** > **Notification Settings**.
3. Select a filter criteria.
4. Optional: Click **Reset** to clear all filter criteria settings.
5. Click .
   The **Filter Criteria** window appears.
6. Edit the log filter criteria.
   For details, see Adding a Log Filter.

7. Click **Apply**.
   All changes are applied.

Removing a log filter

1. Open QuLog Center.
2. Go to **QuLog Service** > **Notification Settings**.
3. Select a filter criteria.
4. Click .
   A confirmation message window appears.
5. Click **Yes**.
   The filter criteria is removed.

17. Notification Center

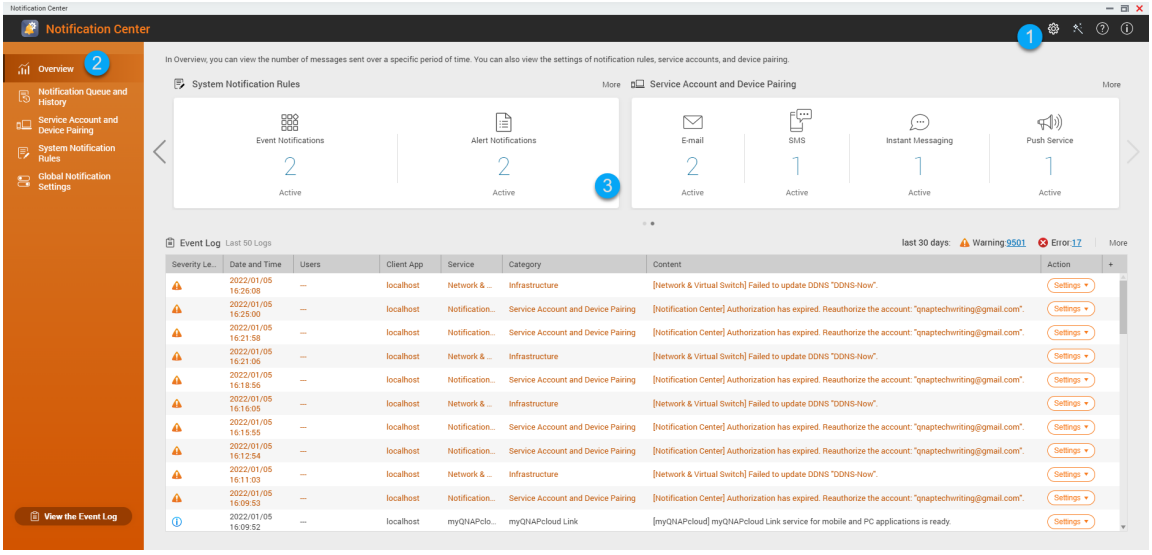
About Notification Center

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.

To send notifications to recipients, you must create custom notification rules, specify the delivery method, and define additional notification criteria in Notification Center. The application supports different delivery channels including emails, SMS, instant messaging, and other push services.

Parts of the user interface

The Notification Center user interface has three main areas.



Label	Area	Description
1	Toolbar	The toolbar displays the following options: • **Settings**: Allows you to send Notification Center data to QNAP. **Important** QNAP does not collect your personal data or information. a. Click  . The **Send Notification data to QNAP** window appears. b. Select **Send Notification data to QNAP**. c. Click **Apply**. • **Quick Start**: Opens the Notification Center guide. • **Help**: Opens the Notification Center Help panel. • **About**: Displays the application version.
2	Menu	The menu allows access to different configuration sections of Notification Center.
3	Main panel	The main panel displays the selected menu option. 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.

Managing notification queue and history

Notification Center allows you to view notification queues and notification history. You can view pending notification messages that Notification Center will send on the **Queue** screen, or go to the **History** screen to view all delivered notification messages.

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 device. You can remove messages at any time before they are sent. Removed messages do not appear on 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. You can also specify how long notification records are retained and where they are stored in **Settings**.

Tasks	User Actions
Export the notification message history.	Click **Export**. Notification Center saves the CSV file on your computer.
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.
Configure the history settings.	1. Click **Settings**. The **Settings** window appears. 2. Specify the maximum number of days to retain notification records before deletion. 3. 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 also configure the SMTP service settings.

Button	Task	User Action
	Send a test message to the specified recipient	1. Click  . 2. Specify an email address. 3. Click **Send**.

Button	Task	User Action
	Edit configurations of an existing email server	1. Click  . The **Edit SMTP Service Account window** appears. 2. Edit the email account settings. 3. Optional: Click **Re-authorization**. The configured email account is authorized again. 4. Optional: Click **Authenticate with Browser Station**. For details, see Pairing Notification Center with a web browser. 5. Optional: Click **Set as the default SMTP service account**. 6. Click **Confirm**.
	Delete an email server	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Configuring an email notification server

1. Go to **Service Account and Device Pairing** > **E-mail**.
2. Click **Add SMTP Service**.
   The **Add SMTP Service** window appears.
3. Select an email account.
4. Configure the following.

Service Providers	User Actions
Outlook	a. Click **Add account**. The email account window appears. b. Specify the email address that will act as the sender for QTS notifications. A confirmation message appears. c. Click **Allow**.

Service Providers	User Actions
Gmail	**a.** Click **Add account**. The email account window appears. **b.** Specify the email address that will act as the sender for QTS notifications. A warning notification appears. **c.** Click **Allow**.
Yahoo	**Important** Before configuring the Yahoo Mail settings, do the following. **a.** Log in to your Yahoo Mail account. **b.** Go to **Help** > **Account Info** > **Account Security**. **c.** Enable **Allow apps that use less secure sign in**. Return to **Notification Center** and specify a valid Yahoo mail address and password.
Custom	**a.** Specify the domain name or the IP address of your SMTP service such as `smtp.gmail.com`. **b.** 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. **c.** Specify the email address that will act as the sender for QTS notifications. **d.** Specify a username that contains a maximum of 128 ASCII characters. **e.** Specify a password that contains a maximum of 128 ASCII characters. **f.** 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**.

> **Note**
> System notifications are sent with the default SMTP service.

6. Optional: Click  .
   The SMTP server sends a test email.
7. Click **Create**.
   Notification Center adds the SMTP service to the list.

SMS notifications

The **SMS** screen allows you to view and configure the short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Vonage (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 configurations of an existing SMS server	1. Click  . The **Edit SMSC Service Account window** appears. 2. Edit the settings. 3. Click **Confirm**.
	Delete an email 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. Select 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
Clickatell - SMS Platform	Clickatell API key
Vonage (Nexmo)	Vonage 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 cannot 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. Click  .
The SMS server sends a test message.

7. Click **Create**.
   Notification Center adds the SMS service to the list.

Instant messaging notifications

The **Instant Messaging** screen allows you to pair Notification Center with instant messaging accounts such as Skype. 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	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure that:

- 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.

Push notifications

The **Push Service** screen allows you to configure push services for web browsers and mobile devices. Notification Center supports pairing the application with multiple third-party push notification services.

Pairing Notification Center with a mobile device

Before pairing, ensure that:

- Your NAS is registered to an active myQNAPcloud account.
- Qmanager iOS 1.8.0 or Qmanager Android 2.1.0 (or later versions) is installed on your mobile device.
- Your NAS is added to 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, click the NAS you want to pair. A confirmation message appears. **b.** Click **Confirm**.
Manual pairing	**a.** Identify your NAS from the device list, and then click  . The device settings screen appears. **b.** Select **Push notifications**. **c.** Click **Save**. A confirmation message appears. **d.** Click **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 that:

- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers:
  - Chrome (version 42 or later)

- Firefox (version 50 or later)

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 up to 127 ASCII characters.
   c. Press **ENTER**.
      Notification Center saves your browser name.

System notification rules

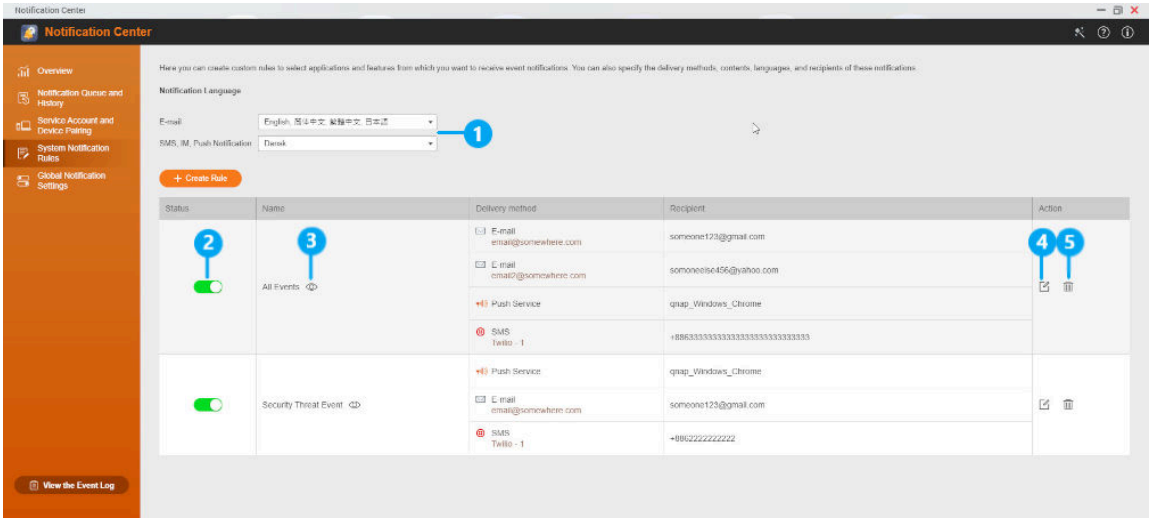
You can create and manage event notification rules in the **Event Notifications** page to receive event notifications promptly.

You can also configure alert notifications to specified recipients in the **Alert Notifications** page by setting the alert severity levels.

Managing event notification rules

The **System Notification Rules** screen allows you to create and customize rules to send notifications to target recipients. To send notifications, you must first create and enable rules that determine which application event triggers the outbound notification. You can customize the message type, delivery method, 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 including emails, SMS, instant messaging, and push services.



Label	Tasks	User Actions
1	Specify a notification language	1. Select one or more languages for email notifications. **Tip** Email notifications contain the notification message repeated in all selected languages. 2. Select a language for SMS, IM, and push notifications.
2	Enable or disable the rule	Click  .
3	Preview 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 a rule	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Creating an event notification rule

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 one or more severity levels.

Severity 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  .

Method	User Action
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 topic: • Pairing Notification Center with Skype
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.

Managing alert notification rules

You can create custom rules to receive alert notifications from the System Logs based on the notification type and keywords in the **Alert Notifications** screen. You can also specify the delivery methods, contents, and recipients of these notifications.

Button	Task	User Action
	Enable or disable the rule	Click  .
	Preview rule settings	1. Click  . The **Alert Notifications** window appears. 2. Review the settings, and then click **Close**.
	Edit the rule	1. Click  . The **Edit Rule for Alert Notifications** window appears. 2. Edit the settings. 3. Click **Confirm**.
	Unpair from and remove the device or browser	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Creating an alert notification rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. 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 severity level.

Severity 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. Optional: 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. Optional: Specify a time range when you want to receive notifications.
6. Optional: 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  .

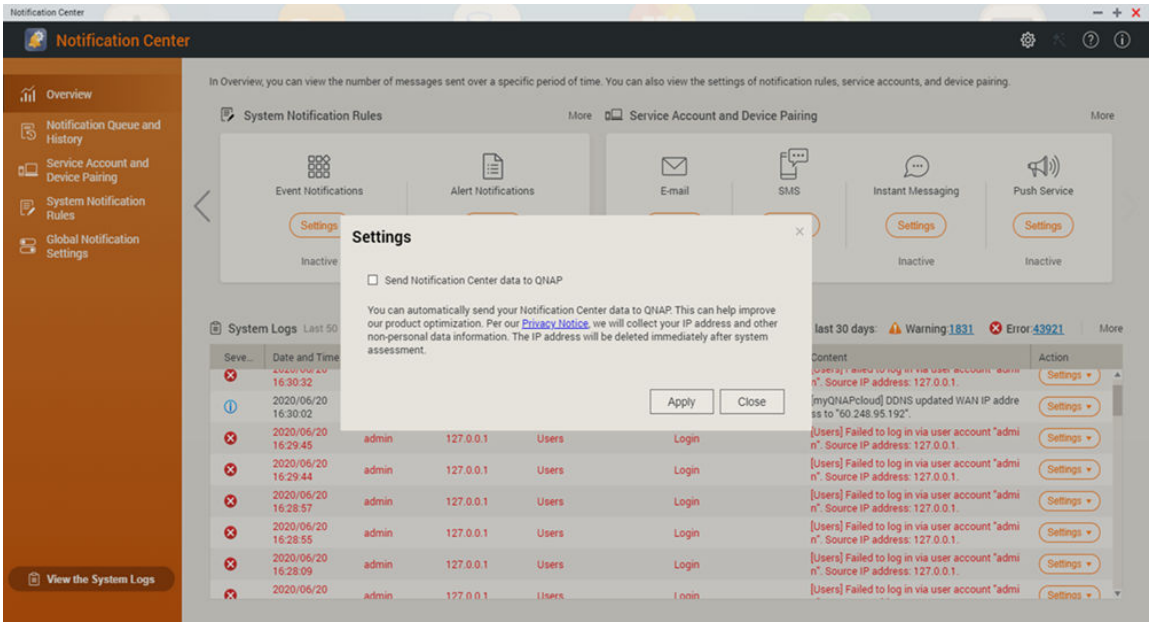
Method	User Action
SMS	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then 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
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.

Settings

The **Settings** screen allows you to enable or disable submitting Notification Center data to QNAP.

Click  to open the **Settings** window.



Enabling the sending of Notification Center data to QNAP

Important

QNAP does not collect your personal data or information.

1. Open **Notification Center**.
2. Click  .
   The **Send Notification data to QNAP** window appears.
3. Select **Send Notification data to QNAP**.
4. Click **Apply**.

Disabling the sending of Notification Center Data to QNAP

Important

QNAP does not collect your personal data or information.

1. Open **Notification Center**.
2. Click  .
   The **Send Notification data to QNAP** window appears.

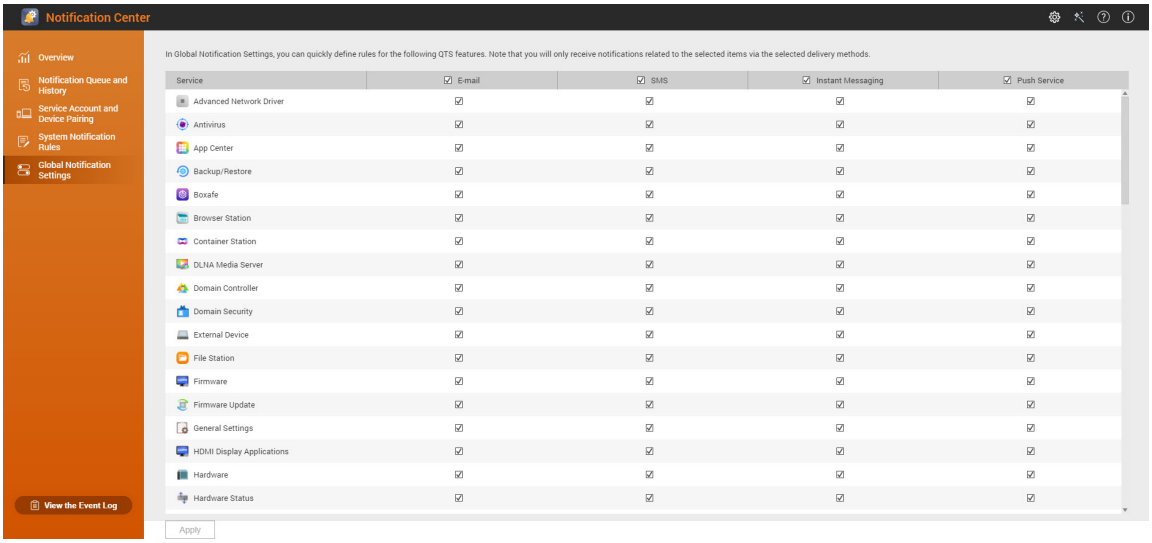
3. Deselect **Send Notification data to QNAP**.
4. Click **Apply**.

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.

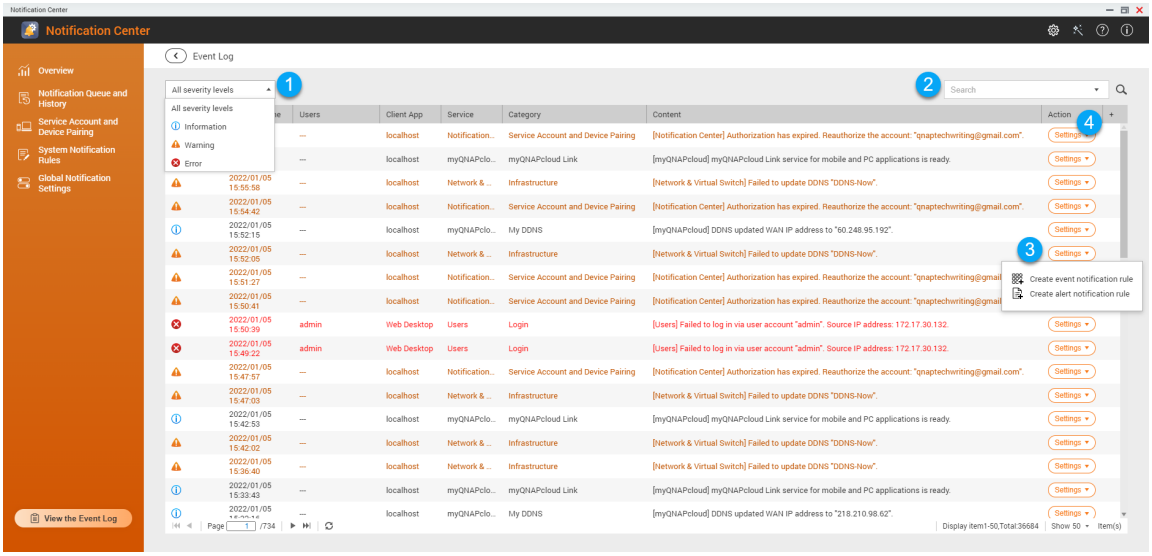
Users only receive notifications related to the selected features through their selected delivery methods.

> **Tip**
> Ensure that you click **Apply** after configuring the global nofitication settings.



Event logs

The **Event Logs** screen displays all the recorded 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 event logs	Select a severity level.
2	Search event logs	Search for logs by keywords or through advanced search. To use advanced search follow the instructions below: **1.** Click ▾ in the search bar. The advanced search option drop down menu appears. **2.** Specify the following parameters where applicable: **Keyword**, **Severity Level**, **Date**, **Users**, **Source IP**, **Application**, **Category**, **Client App**, **Service**. **3.** Click **Search**. Lists all log entries that meet the specified conditions.

No.	Task	User Action
3	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**.
4	Select display items	**1.** Click +. **2.** Select the items to display.

18. Malware Remover

About Malware Remover

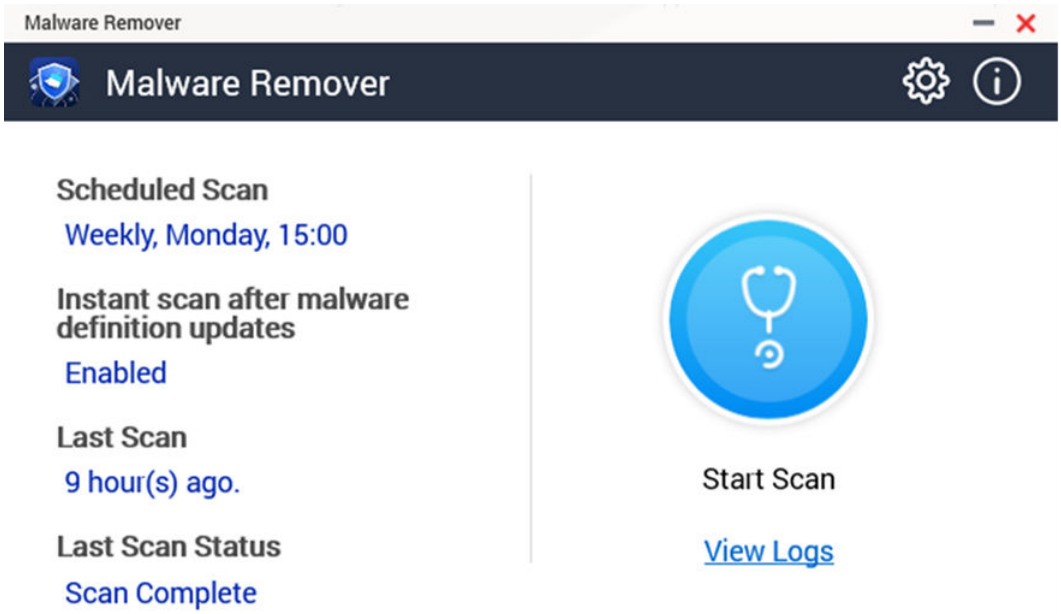
Malware Remover is a built-in utility designed to protect QNAP devices against harmful software. Malware programs are often disguised as or embedded in nonmalicious files and software. They often attempt to gain access to sensitive user information and may negatively impact device performance.

Implementing several layers of protection, Malware Remover allows you to perform instant and scheduled scans on your QNAP device and prevents malicious software from putting your data at risk.

Important
QNAP strongly recommends running routine scans to prevent malware infections and protect the system from advanced risks, threats, and vulnerabilities.

Overview

This screen displays information and controls connected to Malware Remover.



Running a malware scan

1. Open Malware Remover.

2. Click  .
   Malware Remover begins the scan.
3. Optional: After the scan finishes, click **View Logs** to view the results.

Running a scheduled scan

Scheduled scans periodically look for security threats on your QNAP device.

> **Note**
> The **Enable scheduled scan** checkbox is enabled by default.

1. Open Malware Remover.
2. Click  .
3. Choose from the scheduled scan drop-down menu to configure the settings.

Setting	Description
Daily	The scheduled scan runs daily at the specified time.
Weekly	The schedules scan runs once a week on the specified day and time.
Monthly	The scheduled scan runs once a month on the specified date and time.

4. Click **Apply**.

Configuring Malware Remover

1. Open Malware Remover.
2. Click  .
   The **Settings** window opens.
3. Configure the settings.

> **Note**
> All settings are enabled by default to prevent malware threats from infecting the system.

Tip
QNAP recommends running scans during off-peak hours.

Setting	Description
Enable scheduled scan	Enable to scan all applications and files at the user-configured frequency and time. For details, see Running a scheduled scan. **Note** Enabling this setting ensures Malware Remover performs routine scans of your device.
Instant scan after malware definition updates	Enable this option to run instant scans once Malware Remover updates the malware definitions. **Note** Malware Remover automatically updates malware signatures and security patches to have the most up-to-date security content.
Send Malware Remover scan results to QNAP	Enable this option to submit the scan results for malware analysis. QNAP collects data including NAS model, scan status, scan errors, malware detection timestamps, malware ID, and device IP address (the IP address is deleted after analyzing the scan results). **Note** Disabling this option prevents Malware Remover from sending any data to QNAP.

4. Click **Apply**.
Malware Remover saves the settings.

19. Helpdesk

Helpdesk is a built-in application that allows you to quickly find solutions or contact the QNAP support team when you encounter any issues while using QTS and related applications.

Overview

On the **Overview** screen, you can contact the QNAP support team, browse frequently asked questions and application notes, download QNAP user manuals, find out how to use a QNAP devices, search the QNAP knowledge base, and find compatible devices. This screen also displays Helpdesk message logs.

Title	Description
Help Request	Contact the QNAP support team by submitting your issues or questions.
QNAP Online Tutorial & FAQ	Browse frequently asked questions and application notes for QNAP NAS and applications.
User Manual	View or download QNAP user manuals.
QNAP Helpdesk Knowledge Base	Search the QNAP knowledge base for answers from the support team for different issues.
Compatibility List	Find drives and devices that are compatible with QNAP NAS.
My Tickets	View your submitted tickets status.

Configuring settings

1. Open **Helpdesk**.
2. Go to **Overview**.
3. Click .
   The **Settings** window appears.
4. Specify the message retention time.
5. Optional: Click **Retain all messages**.
6. Optional: Click **I am allowing QNAP Support to access my system logs**.
7. Optional: Click **Sign In**.
   The **Settings** window appears.
8. Specify your QNAP ID.
9. Specify the password.

10. Click **Sign In**.
11. Click **Apply**.

Help request

Help Request allows users to directly submit requests to QNAP from your NAS. Helpdesk automatically collects and attaches NAS system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

Submitting a ticket

You can submit a Helpdesk ticket to receive support from QNAP. Helpdesk automatically collects and attaches device system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

1. Open **Helpdesk**.
2. Go to **Help Request**.
3. Sign in with your QNAP ID.
4. Specify the ticket details.

Fields	User Actions
Subject	Specify the subject.
Issue Category	Select an issue category, and then select an issue.
Issue Type	Select an issue type.
Operating System	Select an operating system.
Description	Specify a short description for each issue.

5. Upload the attachments.
   a. Optional: Select **I am allowing QNAP Support to access my system logs**.
   b. Upload screenshots or other related files.

   Note

   - You can upload up to 8 attachments, including system logs.
   - Each file must be less than 5 MB.

6. Specify the following information.

Fields	User Actions
Your Email Address	Specify your email address.
Phone number	Specify your phone number.
Customer type	Select a customer type.
Company name	Specify your company name. **Note** This field only appears when you select Business User as the **Customer type**.
Your timezone	Select a timezone.
Apply the changes to my profile in QNAP Account	Click to apply your profile changes in QNAP Account.
First name	Specify your first name.
Last name	Specify your last name.
Your location	Select a location.

7. Optional: Select **Apply the changes to my profile in QNAP Account**.
8. Click **Submit**.

Remote support

Remote Support allows the QNAP support team to access your NAS directly to assist you with your issues.

Enabling remote support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Specify your ticket ID.
4. Specify your email address.
5. Click **Enable Remote Support**.
   The **QNAP Helpdesk Terms of Service** window appears.

6. Accept the terms of service.
   a. Click **I agree to these Terms of Service**.
   b. Click **Agree**.
      The **Enable Remote Support** window appears.

      Note
      Enable Remote Support is only required when you enable the feature for the first time.

7. Click **Confirm**.
   Helpdesk creates a private key and temporary account.

Extending remote support

Extending Remote Support allows the users to extend the remote session by a week in case users want to have the remote session at a specific time. QNAP will also notify the user to extend the session if the issue is unsolved.

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Extend**.

   Note
   The **Extend** button only appears after Remote Support is enabled.

Disabling remote support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Disable**.

   Note
   The **Disable** button only appears after Remote Support is enabled.

4. Click **Finish**.

   Note
   Remote Support will also be disabled when the support team has completed the remote session, or when the private key has expired.

Diagnostic tool

The Diagnostic Tool provides several features for checking the stability of the NAS. Users can export system kernel records to quickly check whether abnormal operations have recently occurred. In addition, users can send the records to QNAP technical support for further investigation. The Diagnostic Tool also provides features for checking the file system, hard drives, and RAM.

Downloading logs

The Diagnostic Tool provides download log features for checking the device stability. You can export the system kernel records to quickly check for exceptions or errors that have occurred. In addition, you can send the records to QNAP technical support for further investigation.

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool** > **Download Logs**.
3. Click **Download**.
   Helpdesk generates a ZIP file.
4. Download the ZIP file.
5. Optional: Send the file to QNAP through Help Request for further investigation.

Performing an HDD standby test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool** > **HDD Standby Test**.
3. Select an enclosure to analyze.
4. Click **Start**.
   Helpdesk performs an HDD standby test.
5. Optional: Click **Download** to download the test reports.

Performing an HDD stress test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool** > **HDD Stress Test**.
3. Click **Start**.
   Helpdesk performs an HDD stress test.
4. Optional: Click **Download** to download the test reports.

20. Console Management

Console Management is a text-based tool that helps system administrators perform basic configuration or maintenance tasks, and provide technical support to the NAS users. The program is accessible only after the operating system has finished initialization. Console Management is enabled by default, but you can disable it in the Control Panel. For details, go to the System Settings section of the QTS User Guide. Currently, disabling Console Management only applies to QTS.

Only users in the administrator group can use Console Management, which launches automatically when administrators log in using SSH login, a serial console, or an HDMI monitor and a USB keyboard.

Enabling Secure Shell (SSH)

Secure Shell (SSH) is a cryptographic network protocol that can access Console Management. If you want to access Console Management using SSH, you must first enable SSH on the NAS.

Enabling SSH on the NAS

1. Log in to the NAS as administrator.
2. Go to **Control Panel** > **Network & File Services** > **Telnet / SSH**.
3. Select **Allow SSH connection (Only administrators can login remotely.)**.
4. Optional: Change the port number.
5. Click **Apply**.

Enabling SSH on the NAS using Qfinder Pro

1. Open **Qfinder Pro**, and then locate the NAS you want to access.
2. Click **Settings**.
3. Select **Connect via SSH**.
   The **Connect via SSH** screen appears.
4. Log in to the NAS as administrator.

Accessing Console Management

Before you can access Console Management, you must first enable SSH using the NAS or Qfinder Pro. A third-party software is also required on Windows platforms but not on Mac platforms.

Accessing Console Management from Windows

1. Download PuTTY from https://www.putty.org and then follow the on-screen instructions to install the software.
2. Open PuTTY, and type the device's IP address underneath **Host Name (or IP address)**.

3. Select **SSH** as the connection type.

   Note
   This option is selected by default.

4. Click **Open**.
   The **PuTTY Security Alert** window appears.

   Note
   This window only appears when you first run the application.

5. Click **Yes**.
   A login screen appears.

Accessing Console Management from Mac

1. Open **Terminal**.
2. Enter `ssh USERNAME@NAS_IP`.

   Note
   Replace `NAS_IP` with the device's IP address.

   Tip
   If you encounter an error, enter `ssh-keygen -R NAS_IP`. Replace `NAS_IP` with the device's IP address.

3. Press **ENTER**.
   A login screen appears.

Logging In to Console Management

Important

Before performing this task, you must first complete the following tasks:

- Enable Secure Shell (SSH).
- Download the third-party software for your platform if it is required. For details, see the following topics:
  - Accessing Console Management from Windows
  - Accessing Console Management from Mac

1. Log in as administrator.
   a. Enter the username.
   b. Enter the password.

   Note

   For security purposes, the password does not show.

   Tip

   Do not copy and paste the password to the program.

   The **Console Management - Main menu** screen appears.

Managing existing applications

1. Log in to Console Management, and then enter `5`.
   The App window and three options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

   Tip

   To browse your applications, enter `n` or `p` to go to the next or previous page.

Option	User Action
List installed apps	Enter `1`. Console Management displays a list of all installed applications on the operating system.

Option	User Action
List enabled apps	Enter `2`. Console Management displays a list of all enabled applications on the operating system.
List disabled apps	Enter `3`. Console Management displays a list of all disabled applications on the operating system.
Return	Enter `r`. Console Management returns to Main menu.

A list of applications appear.

3. Enter the alphanumeric character corresponding with the application you want to perform an action on.
   Five options appear.
4. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Start	Enter `1`. The application starts.
Stop	Enter `2`. The application stops.
Restart	Enter `3`. The application restarts.
Remove	Enter `4`. The application is removed. **Note** If an application can't be removed, Console Management tells you that this function is currently unavailable.
Return	Enter `r`. Console Management returns to Main menu.

The system performs the specified action and tells you whether the action has succeeded or not.

Activating or deactivating a license

1. Log in to Console Management, and then enter `4`.
   Two options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Activate a License	**a.** Enter `1`. **b.** Enter a license activation key.
Deactivate a License	**a.** Enter `2`. **b.** Enter a license activation key.
Return	Enter `r`. Console Management returns to Main menu.

The system performs the specified action.

Sorting and filtering system logs

1. Log in to Console Management, and then enter `2`.
   Eleven options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

> **Note**
> System logs are displayed in the following format: record_id, date, time, user, app_id, application, category_id, category, msg_id, message.

Option	User Action
date in ascending order	Enter `1`. Console Management displays all system logs in ascending order according to the date.
date in descending order (default)	Enter `2`. Console Management displays all system logs in descending order according to the date.
user in ascending order	Enter `3`. Console Management displays all system logs in ascending order according to the username.

Option	User Action
user in descending order	Enter `4`. Console Management displays all system logs in descending order according to the username.
IP in ascending order	Enter `5`. Console Management displays all system logs in ascending order according to the IP address.
IP in descending order	Enter `6`. Console Management displays all system logs in descending order according to the IP address.
app name in ascending order	Enter `7`. Console Management displays all system logs in ascending order according to the application name.
app name in descending order	Enter `8`. Console Management displays all system logs in descending order according to the application name.
category in ascending order	Enter `9`. Console Management displays all system logs in ascending order according to the application category.
category in descending order	Enter `10`. Console Management displays all system logs in descending order according to the application category.

The filter screen appears.

3. Optional: Enter a filter query.

Note

- Ensure all filter conditions follow the relevant on-screen format. For example, filtering by an application name should follow this format: `A={myQNAPcloud}`.
- To filter by multiple conditions, use '&' in between filters. For example, filtering by severity level and an application name should follow this format: `T={0}&A={myQNAPcloud}`.

Filter	User Action
Severity level	**a.** Enter one of the following options. • `T={0}` **Note** This filter only includes system logs classified as information. This type of system log is indicated as ⓘ in QuLog Center. • `T={1}` **Note** This filter only includes system logs classified as warnings. This type of system log is indicated as ⚠ in QuLog Center. • `T={2}` **Note** This filter only includes system logs classified as errors. This type of system log is indicated as ⛔ in QuLog Center. Console Management filters all system logs according to the specified severity level.
Keyword	Enter a keyword. Console Management filters all system logs according to the specified keyword.
Username	Type an username. Console Management filters all system logs according to the specified username.
Source IP	Enter a source IP. Console Management filters all system logs according to the specified source IP.
Application name	Enter an application name. Console Management filters all system logs according to the specified application name.

Filter	User Action
Category name	Enter an application category. Console Management filters all system logs according to the specified category.

A list of system logs appear.

Tip
To browse your applications, enter `n` or `p` to go to the next or previous page.

Showing network settings

1. Log in to Console Management as administrator, and then enter `1`.

   Note
   Network settings appear in the following format: adapter, virtual switch, status, IP, MAC address.

   The Network settings window appears.

Restoring or reinitializing the device

1. Log in to Console Management as administrator, and then enter `3`.
   The **Reset** window and five options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

   Note
   The admin password is required to reset the settings or reinitialize the device.

Option	User Action
Reset network settings	Enter `1`. Console Management resets the network settings.
Reset system settings	Enter `2`. Console Management restores system settings to default without erasing user data.
Restore factory defaults & format all volumes	Enter `3`. Console Management restores the system settings to default and formats all disk volumes.

Option	User Action
Reboot to reinitialize the device	Enter `4`. Console Management erases all data and reinitializes the device.
Return	Enter `r`. Console Management returns to Main menu.

Rebooting the NAS

You can reboot the NAS into rescue or maintenance mode from Console Management.

Rebooting the device into rescue mode

1. Log in to **Console Management** as administrator, and then type `6` and press **ENTER**.
   The **Reboot in rescue mode** window opens.
2. Type `y`, and then press **ENTER**.

   Note
   Press escape or type `n` and press to go to the **Main Menu**.

   Console Management reboots the device.

Rebooting the device into maintenance mode

1. Log in to **Console Management** as administrator, and then type `7` and press **ENTER**.
   The **Reboot in maintenance mode** window opens.
2. Type `y`, and then press **ENTER**.
   Press escape or type `n` and press to go to the **Main Menu**.
   Console Management reboots the device.