QuTS hero h6.0.x

User Guide

Document version: 1
09/04/2026

Contents

1. Overview

About QuTS hero 13
What's New in QuTS hero 13
QuTS hero initialization 14
Initializing QuTS hero using Qfinder Pro 14
Initializing QuTS hero using the cloud installation website 16
NAS access 19
Accessing the NAS using a browser 20
Accessing the NAS using Qfinder Pro 21
Accessing the NAS using Qmanager 21
QuTS hero navigation 22
Task Bar 22
Main Menu 32
Desktop 35
Login and Security 41
Password management 42
2-step verification 43
Passwordless login 54
Login with a QNAP ID 59
Login with a Passkey 60
High Availability 61
Support and other resources 61

2. Getting Started

Storing data 62
Accessing data 62
Backing up data 63
Configuring privilege settings 64
Setting up remote access 64
Acquiring apps and licenses 65
Securing the NAS 65

3. System Settings

General settings 68
Configuring system administration settings 68
Configuring time settings 70
Configuring daylight saving time 71
Configuring codepage settings 72
Configuring region settings 72
Configuring the login screen 72
Configuring console management 73
Security 73
Configuring the allow/deny list 73
Configuring IP access protection 74

Configuring account access protection....75
SSL certificate & private key....75
Configuring the password policy....78
KMIP service....79
Hardware....84
Configuring general hardware settings....84
Configuring audio alert settings....85
Configuring the backup battery unit (BBU) settings....86
Configuring smart fan settings....86
Configuring hardware resource settings....87
Power....90
Configuring EuP mode....90
Enabling or disabling Wake-on-LAN (WOL)....91
Configuring the power recovery settings....91
Configuring the power schedule....91
Firmware update....92
Firmware update requirements....93
Checking for updates....94
Updating the firmware automatically....95
Updating the firmware manually....98
Updating the firmware using Qfinder Pro....99
System backup and restore....100
Backing up system settings....100
Restoring system settings....102
System reset and restore to factory default....106
External device....109
Uninterruptible power supply (UPS)....109
Configuring USB settings....112
System status....113
Resource Monitor....113

4. Privilege Settings

Users....115
Default administrator account....115
Creating a local user....118
Creating multiple users....121
User account lists....122
Importing users....124
Exporting users....126
Modifying user account information....126
Deleting users....129
Home folders....130
User groups....130
Default user groups....130
Creating a user group....130
Modifying user group information....132
Deleting user groups....133
Delegated administration....133
Delegated roles and permission restrictions....133

Assigning delegated roles to users 136
Removing delegated roles from users 137
Viewing user permissions 137
Exporting a delegation list 138
Importing a delegation list 138
Shared folders 139
Default shared folders 139
Creating a shared folder 140
Editing shared folder properties 147
Refreshing a shared folder 150
Removing shared folders 150
ISO shared folders 151
Shared folder permissions 153
Folder aggregation 159
Shared folder encryption 162
Shared folder access 164
Quota 170
Enabling quotas 171
Editing quota settings 171
Exporting quota settings 172
Quota conflicts 172
Domain security 173
Active Directory (AD) authentication 173
Microsoft Entra single sign-on (SSO) 177
LDAP authentication 178
AD and LDAP management 181
Domain controller 183
Enabling a domain controller 183
Resetting a domain controller 185
Default domain user accounts 185
Creating a domain user 185
Creating multiple domain users 186
Domain user account lists 188
Modifying domain user account information 190
Deleting domain users 191
Domain user groups 191
Computers 193
DNS 195
Back up/restore 199

5. Services

Antivirus 201
Enabling antivirus 201
Scanning shared folders 202
Managing scan jobs 204
Managing reported scan jobs 204
Managing quarantined files 205
Servers 206
Web server 206

LDAP server ... 209
MariaDB server ... 211
Syslog server ... 217
RADIUS server ... 220
Enabling the TFTP server ... 223
Enabling the NTP server ... 223

6. File Station

About File Station ... 225
System requirements ... 225
File Station user interface ... 225
Supported file formats ... 229
File and folder operations ... 230
Uploading files and folders ... 232
Downloading files and folders ... 233
Viewing file or folder properties ... 234
Opening a file ... 234
Opening Microsoft Word, Excel, and PowerPoint files using the Chrome extension ... 235
Opening a text file using text editor ... 236
Viewing a file in Google Docs ... 236
Viewing a file in Microsoft Office Online ... 237
Opening image files using Image2PDF ... 237
Viewing storage information ... 238
Viewing Qsync folders ... 238
Managing share links ... 239
Viewing files and folders shared with me ... 240
Sorting files and folders ... 240
Copying files and folders ... 240
Moving files and folders ... 242
Renaming files or folders ... 243
Compressing files and folders ... 244
Extracting compressed files or folders ... 245
Deleting a file ... 246
Restoring a deleted file ... 246
Encrypting files ... 247
Decrypting files ... 248
Mounting an ISO file ... 249
Unmounting an ISO file ... 249
Creating a folder ... 249
Creating a desktop shortcut ... 250
Adding a folder to Favorites ... 251
Removing a folder from Favorites ... 251
Sharing a file or folder by email ... 252
Sharing a file or folder on a social network ... 255
Sharing a file or folder using share links ... 257
Sharing a file or folder with a NAS user ... 259
Creating a shared folder ... 262
Playing an audio file ... 269
Playing a video file ... 270

Playing a video file using CAYIN Media Viewer....271
Locking or unlocking an encrypted shared folder....271
Opening a 360-degree image or video file....272
Adding a file or folder to the transcoding folder....273
Canceling or deleting transcoding....274
Viewing transcode information....275
Keeping a folder or a file in reserved cache....275
Converting Apple iWork files to Microsoft Office files....276
Removing a folder from reserved cache....277
Viewing file properties....278
File Station searches....279
Searching for files and folders....279
Using Qsirch mode to search for file content....280
Other tasks....280
Removing background tasks....280
Modifying general settings....281
Modifying file transfer settings....282
Modifying multimedia settings....283
Modifying document settings....284
Modifying file operations settings....286
Modifying third-party service settings....286

7. Storage Manager

QNAP flexible storage architecture....287
Global settings....288
Storage global settings....288
Disk health global settings....290
Storage....291
Disks....291
Storage pools....303
Qtier hero storage pools....324
Shared folders....335
RAID....352
Self-encrypting drives (SEDs)....358
Expansion units....366
Expansion unit actions....366
Expansion unit recovery....367
QNAP external RAID devices....367
QNAP JBOD enclosures....378
Licensing for third-party expansion units....380
Cache acceleration....380
Cache acceleration requirements....380
Creating the SSD cache....381
Configuring SSD cache disks....384
Configuring cached storage....384
Removing the SSD cache....385
External storage....385
External storage device actions....385
External storage partition actions....386

Formatting an external storage disk or partition..... 386
Remote disk..... 388
Remote disk limitations..... 388
Adding a remote disk..... 388
Remote disk and iSCSI target actions..... 390
VJBOD (Virtual JBOD)..... 391
VJBOD requirements..... 392
VJBOD limitations..... 392
VJBOD automatic reconnection..... 392
VJBOD creation..... 393
VJBOD management..... 398
VJBOD Cloud..... 401
Installing VJBOD Cloud..... 401
VJBOD Cloud volume and LUN creation..... 402
VJBOD Cloud management..... 416
Transfer resources..... 420
Event logs..... 422
VJBOD Cloud licenses..... 422

8. Snapshot Manager

Snapshots..... 424
Snapshot storage limitations..... 424
Snapshot global settings..... 424
Snapshot creation..... 426
Taking a snapshot..... 426
Configuring a snapshot schedule..... 428
Snapshot management..... 432
Editing a snapshot..... 432
Editing a snapshot schedule..... 433
Viewing snapshot details..... 436
Configuring a snapshot retention policy..... 436
Importing a snapshot..... 437
Exporting a snapshot..... 438
Deleting snapshots..... 439
Calculating snapshot size..... 439
Configuring pool guaranteed snapshot space..... 440
Snapshot data recovery..... 441
Restoring files and folders from a snapshot..... 441
Restoring files and folders from a snapshot vault..... 442
Reverting a shared folder from a snapshot..... 443
Reverting a LUN from a snapshot..... 444
Restoring files and folders using Windows Previous Versions..... 446
Snapshot cloning..... 446
Regular clone and Instant Clone..... 446
Cloning a shared folder from a snapshot..... 447
Cloning a shared folder from a snapshot vault..... 448
Cloning a LUN from a snapshot..... 449
Cloning a LUN from a snapshot vault..... 451
Snapshot Replica..... 452

Protection levels....452
Snapshot Replica requirements....453
Creating a Snapshot Replica job....454
Managing a Snapshot Replica job....458
Snapshot vaults....459
Managing a snapshot vault....459
Importing vault data from a remote Snapshot Replica source....460
SnapSync....460
SnapSync requirements....461
SnapSync limits and restrictions....461
Creating a SnapSync job with a remote NAS as destination....462
SnapSync management....466
QNAP Snapshot Agent....472

9. iSCSI & Fibre Channel

Storage limits....473
iSCSI storage limits....473
Fibre Channel storage limits....473
iSCSI & Fibre Channel global settings....473
LUNs....475
Creating a block-based LUN....475
Managing LUN encryption....481
LUN actions....484
LUN status....485
LUN import and export....486
iSCSI....489
Getting started with iSCSI....489
iSCSI performance optimization....489
iSCSI targets....490
iSCSI access control list....497
iSCSI target authorization....499
Fibre Channel....500
Getting started with Fibre Channel....500
Fibre Channel ports....500
Fibre Channel port groups....502
Fibre Channel LUN masking....505
Fibre Channel WWPNs....507
NPIV service for high-availability clusters....508

10. ZFS Pool Profiling Tool

Installing ZFS Pool Profiling Tool....510
Storage pool over-provisioning....510
Creating a storage pool over-provisioning test....510
Test reports....512
Settings....513

11. Network & Virtual Switch

About Network & Virtual Switch....514
Parts of the user interface....514

Basic network adapter configuration....516
Configuring IPv4 settings....517
Configuring IPv6 settings....518
Configuring the system default gateway....519
Configuring static route settings....520
Configuring IEEE 802.1X authentication....522
IP addressing services configuration....524
Configuring DNS server settings....524
Configuring DHCP server settings....525
Adding DHCP clients to a DHCP server....527
Configuring RADVD server settings....529
Configuring DDNS service settings....531
LAN switching configuration....532
Configuring VLAN settings....532
Configuring port trunking settings....533
Virtual switch configuration....534
Creating a virtual switch in basic mode....535
Creating a virtual switch in advanced mode....536
Creating a virtual switch in software-defined switch mode....540
Network policies configuration....540
Configuring Forward Error Correction (FEC) settings....540
Wireless network configuration....541
Adding a wireless network....541
Enabling Wi-Fi....543
Connecting to a wireless network....544
Understanding the wireless connection messages....549
Accessing the wireless access point (AP) settings....549
USB QuickAccess configuration....550
Enabling USB QuickAccess....550
Configuring the USB QuickAccess IP address....551
Configuring USB QuickAccess authentication....551
Thunderbolt interface configuration....552
Enabling T2E with Qfinder Pro....552
Enabling T2E on macOS....553
Updating the firmware of a network expansion card....553

12. Network & File Services

About Network & File Services....555
QNAP service ports....555
Network access settings....557
Configuring service binding settings....558
Configuring proxy server settings....558
Configuring reverse proxy rule settings....559
Modifying reverse proxy rules....561
Network protocol settings....562
Configuring telnet connections....562
Configuring SSH connections....562
Editing SSH access permissions....563
Configuring SNMP settings....563

Downloading the SNMP MIB....565
File sharing protocol settings....565
Configuring Samba (Microsoft networking) settings....565
Configuring network binding and SMB multichannel settings....569
Configuring AFP (Apple networking) settings....570
Configuring NFS service settings....570
Accessing FTP (QuFTP Service) settings....573
Configuring WebDAV settings....573
Service discovery settings....576
Enabling the UPnP discovery service....576
Enabling the Bonjour discovery service....576
Enabling the Qfinder discovery service....577
Recycle Bin management....577
Configuring the Recycle Bin settings....577
Deleting all files in the Recycle Bin....578
Restricting access to the Recycle Bin....578

13. myQNAPcloud

Initial setup....579
Creating a QNAP ID....579
Creating an organization....580
Setting up myQNAPcloud and AMIZ Cloud for the NAS....581
Basic operations and service statuses....582
Access management....583
Configuring device access controls for stand-alone devices....584
Configuring device access controls for organization devices....584
Enabling myQNAPcloud Link....585
Restoring the AMIZ Cloud Agent connection....585
Configuring DDNS settings....585
Installing an SSL certificate....586

14. App Center

Navigation....589
Left panel....589
Toolbar....589
Main area....590
App management....591
Viewing app information....591
Buying an app license....592
Installing an app from App Center....593
Installing an app manually....593
Updating an app....594
Batch updating multiple apps....595
Enabling or disabling an app....595
Migrating an app....595
Granting or denying user access to an app....596
Uninstalling an app....596
Viewing apps installed on other devices....597
App Center settings....597

Adding an app repository....597
Configuring app update settings....598
Digital signatures....599
Enabling installation of apps without digital signatures....599

15. Licenses

About QNAP licenses....600
License types and plans....600
Validity period....601
License portals and utility....601
Software Store....601
License Center....602
License Manager....602
Buying a license using QNAP ID....602
License activation....603
Activating a license using QNAP ID....604
Activating a license using a license key....607
Activating a license using a product key or PAK....608
Activating a license offline....609
License deactivation....610
Deactivating a license using QNAP ID....610
Deactivating a license offline....611
License extension....612
Extending a license using QNAP ID....613
Extending a license offline using an unused license....614
Extending a license offline using a product key....615
Upgrading a license....616
Viewing license information....618
Recovering licenses....619
Transferring a license to the new QNAP license server....619
Deleting a license....620

16. Multimedia

HybridDesk Station (HD Station)....621
Installing HD Station....622
Configuring HD Station....623
HD Station applications....624
Using HD Player in HD Station....624
DLNA Media Server....625
Enabling and configuring DLNA media server....625
Configuring DLNA Media Server....625
Media Streaming Add-on....625
Configuring general settings....626
Configuring browsing settings....627
Configuring media receivers....628
Multimedia Console....628
Overview....628
Content Management....629
Indexing....630

Thumbnail generation....631
Transcoding....634
Multimedia app suite....640

17. QuLog Center

Monitoring logs....644
Event log....644
Access logs....645
Local device logs....646
Local event logs....646
Local access logs....649
Online users....652
Creating a custom filter tab for local device logs....653
Local log settings....657
QuLog Service....663
Configuring log sender settings....663
Configuring log reciever settings....665
Viewing and managing remote logs....668
Notification settings....679
Configuring notification rule settings....679
Adding a log filter....680
Editing a log filter....680
Removing a log filter....681

18. Notification Center

About Notification Center....682
Parts of the user interface....682
Managing notification queue and history....683
Service account and device pairing....684
Email notifications....684
SMS notifications....688
Push notifications....690
System notification rules....691
Managing event notification rules....691
Creating an event notification rule....693
Managing alert notification rules....696
Creating an alert notification rule....696
Settings....699
Enabling the sending of Notification Center data to QNAP....700
Disabling the sending of Notification Center Data to QNAP....700
Global notification settings....701
Event logs....701

19. Malware Remover

About Malware Remover....704
Overview....704
Running a malware scan....704
Running a scheduled scan....705
Configuring Malware Remover....705

Enabling Ransomware Guard 706
Managing quarantined items 707

20. Helpdesk

Overview 709
Configuring settings 709
Help request 710
Submitting a ticket 710
Remote support 711
Enabling Remote Support 711
Extending remote support 712
Disabling remote support 712
Diagnostic Tool 713
Downloading logs 713
Performing an HDD standby test 713
Performing an HDD Stress Test 713

21. Console Management

Enabling Secure Shell (SSH) 714
Enabling SSH on the NAS 714
Enabling SSH on the NAS using Qfinder Pro 714
Accessing Console Management 714
Accessing Console Management from Windows 714
Accessing Console Management from Mac 715
Logging In to Console Management 716
Managing existing applications 716
Activating or deactivating a license 718
Sorting and filtering system logs 718
Showing network settings 721
Restoring or reinitializing the device 721
Rebooting the NAS 722
Rebooting the device into rescue mode 722
Rebooting the device into maintenance mode 722

1. Overview

About QuTS hero

QuTS hero 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. QuTS hero also has built-in utilities that extend the functionality and improve the performance of the NAS.

QuTS hero uses the advanced ZFS file system, which offers features such as inline data duplication, compression, compaction, self healing, and multi-level caching to ensure data integrity and high performance.

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

What's New in QuTS hero

To see more new features and enhancements, go to https://www.qnap.com/go/release-notes/.

QuTS hero h6.0.x

- QuTS hero now supports creating a high-availability environment clusters to ensure continuous service availability in the event of hardware failures. For more information, see the High Availability Manager User Guide: https://docs.qnap.com/application/ha-manager/1.x/en-us
- The LCD panel on NAS devices can now display high-availability (HA) information when the devices are in an HA cluster, including cluster name, node role, and cluster IP address.
- The status LED on NAS devices can now indicate high-availability (HA) statuses when the devices are in an HA cluster: solid green for the active node role, blinking green for the passive node role, and solid red for HA errors.
- You can now make your snapshots immutable for extra protection against accidental modifications or malicious tampering such as ransomware attacks.
- QuTS hero now supports FIDO2 (Fast Identity Online 2), which is an authentication standard that strengthens account security and provides a smoother login experience. With FIDO2, you can log in to the NAS with more secure methods such as Windows Hello, Touch ID, and hardware authentication devices such as YubiKey.
- You can now log in to the NAS with your QNAP ID to streamline your login experience. To do so, you can link your QNAP ID to a local or domain account for a NAS device.
- Added support for enabling KMIP (Key Management Interoperability Protocol) service. By configuring a KMIP client and connecting it to a remote key server of your choice, you can securely store and access your encryption keys for various NAS features, such as encrypted shared folders and encrypted LUNs.

- iSCSI & Fibre Channel now supports N_Port ID Virtualization (NPIV), a Fibre Channel (FC) technology that allows multiple World Wide Names (WWNs) to share a single physical port.
- Storage Manager now supports the creation of Qtier storage pools to improve storage efficiency and enhance read/write performance. Each pool can include two to three tiers, with faster tiers for frequently accessed data and slower tiers for less frequently accessed data.
- Malware Remover now introduces Ransomware Guard, a feature that strengthens system security by detecting and controlling suspicious programs. Ransomware Guard monitors unusual behaviors such as unauthorized file encryption, file renaming, and excessive read/write activity, and can automatically restrict programs that match known malware signatures.
- QuTS hero now supports upgrading ACL (Access Control List) to 2.0 to enhance ACL performance. This upgrade significantly improves the performance of checking or configuring permission settings for a large number of files and folders. In addition, it also increases the limit of configurable ACL entries, thus further enhancing permission management flexibility for larger organizations.
- Storage & Snapshots are now divided into Storage Manager and Snapshot Manager to streamline task workflow and enhance user experience.
- LUN import and export jobs now support using a remote folder mounted via HybridMount as job destination. For details, see: https://www.qnap.com/go/how-to/faq/con_show.php?cid=3184
- You can now use your local NAS as a destination for exporting snapshots.
- You can now configure snapshot access settings and remote Snapshot Replica connection timeout settings in **Snapshot Manager** > **Global Settings**
- Snapshots now have a "protection policy" attribute that combines the previous feature of permanent snapshots and the property of immutability. When taking or editing a snapshot, or configuring a local snapshot schedule, you can now select a protection policy that prohibits automatic deletion by the system and/or manual deletion by a user. You can also specify the prohibition expiration time.

QuTS hero initialization

Initializing QuTS hero using Qfinder Pro

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

Warning
Installing QuTS hero deletes all data on the drives. Back up your data before proceeding.

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

3. Run Qfinder Pro on a computer that is connected to the same local area network.

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

4. Locate the NAS in the list and then double-click the name or IP address.
   The **Smart Installation Guide** opens in the default web browser.

5. If the screen shows a different operating system, click **QuTS hero**.

   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 QuTS hero.

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

6. Click **Start Smart Installation Guide**.
   The **Install Firmware** window appears.

7. Install firmware using any of the following methods:

Installation methods	Steps
Automatic	Click **Start**. Automatically searches for available firmware updates and installs firmware.
Manual installation	**a.** Click **Manual Installation**. The **Install Firmware** window appears. **b.** Click **Browse**. The upload file window appears. **c.** Select file. **d.** Click **Open**. Starts firmware installation.
Skip	Click **Skip**. Skips firmware installation.

8. Specify the following information

   - **NAS name**: Specify a name with 1 to 14 characters. The name supports 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 protect your NAS from brute force attacks, create a new system administrator account during QuTS hero initialization to disable the default "admin" account.

- **Password**: Specify an administrator password with 1 to 64 characters. The password supports all ASCII characters.

9. Click **Next**.
10. Specify the time zone, date, and time.

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

11. Click **Next**.
    The **Configure the network settings** screen appears.
12. Select **Obtain an IP address automatically (DHCP)**.
13. Click **Next**.
14. Review the settings.
15. Click **Apply**.
    A confirmation message appears.

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

16. Click **Initialize**.
    QuTS hero initialization starts. It may take a few minutes to complete the process.
    After the initialization, you can click **Go to NAS Management** to start using QuTS hero and configuring other settings.

Initializing QuTS hero using the cloud installation website

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

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

1. Power on the device.
2. Connect the device 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 QuTS hero through LAN and then installing myQNAPcloud Link.
7. Click **Next**.
   The **Smart Installation Guide** opens in the default web browser.
8. Perform any of the following actions.
   - To check for the latest available version, click **Start**.
     The wizard downloads the latest available version, and then the NAS restarts after the download is complete. If a newer version is not available, the wizard automatically displays the **Smart Installation Guide**.
   - To install the out-of-the-box version, click **Skip**.
   - If the screen shows a different operating system, click **QuTS hero**.

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

9. Click **Start Smart Installation Guide**.
   The **Install Firmware** window appears.
10. Install firmware using any of the following methods:

Installation methods	Steps
Automatic	Click **Start**. Automatically searches for available firmware updates and installs firmware.
Manual installation	**a.** Click **Manual Installation**. The **Install Firmware** window appears. **b.** Click **Browse**. The upload file window appears. **c.** Select file. **d.** Click **Open**. Starts firmware installation.
Skip	Click **Skip**. Skips firmware installation.

11. Specify the following information

    - **NAS name**: Specify a name with 1 to 14 characters. The name supports 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 protect your NAS from brute force attacks, create a new system administrator account during QuTS hero initialization to disable the default "admin" account.

    - **Password**: Specify an administrator password with 1 to 64 characters. The password supports all ASCII characters.
12. Click **Next**.

13. Specify the time zone, date, and time.

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

14. Click **Next**.
    The **Configure the network settings** screen appears.
15. Select **Obtain an IP address automatically (DHCP)**.
16. Click **Next**.
17. Review the settings.
18. Click **Apply**.
    A confirmation message appears.

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

19. Click **Initialize**.
    QuTS hero initialization starts. It may take a few minutes to complete the process.
    After the initialization, you can click **Go to NAS Management** to start using QuTS hero and configuring other settings.

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

Method	Description	Requirements
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
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 QuTS hero login screen appears.
4. Optional: Log in QuTS hero using HTTPS.
   a. Select **Secure login**.
      A confirmation message appears.
   b. Click **OK**.
      You will be redirected to the QuTS hero 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 Microsoft Entra single sign-on (SSO).

The QuTS hero 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 QuTS hero login screen opens in the default web browser.
4. Specify your username and password.
5. Click **Login**.
   The QuTS hero 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.

QuTS hero navigation

There are several methods for navigating QuTS hero. 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. **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.

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.

No.	Element	Possible User Actions

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**.

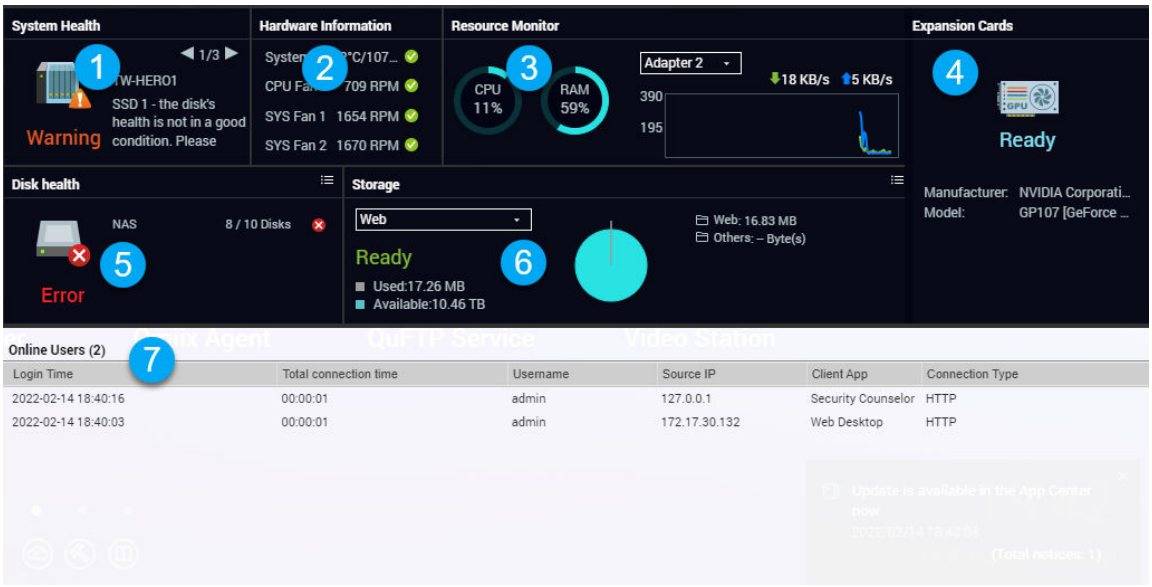
No.	Element	Possible User Actions
9	**[USER_NAME]**	Click the button to view the last login time and the following menu items: • **Language**: Opens a list of supported languages and allows you to change the language of the operating system • **Desktop Preferences**: Opens a list of display modes and 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 QuTS hero 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
		• **Customer Service**: Opens the **QNAP Customer Service** 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 pool name
		  • Used disk space
		  • Available disk space

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.

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.

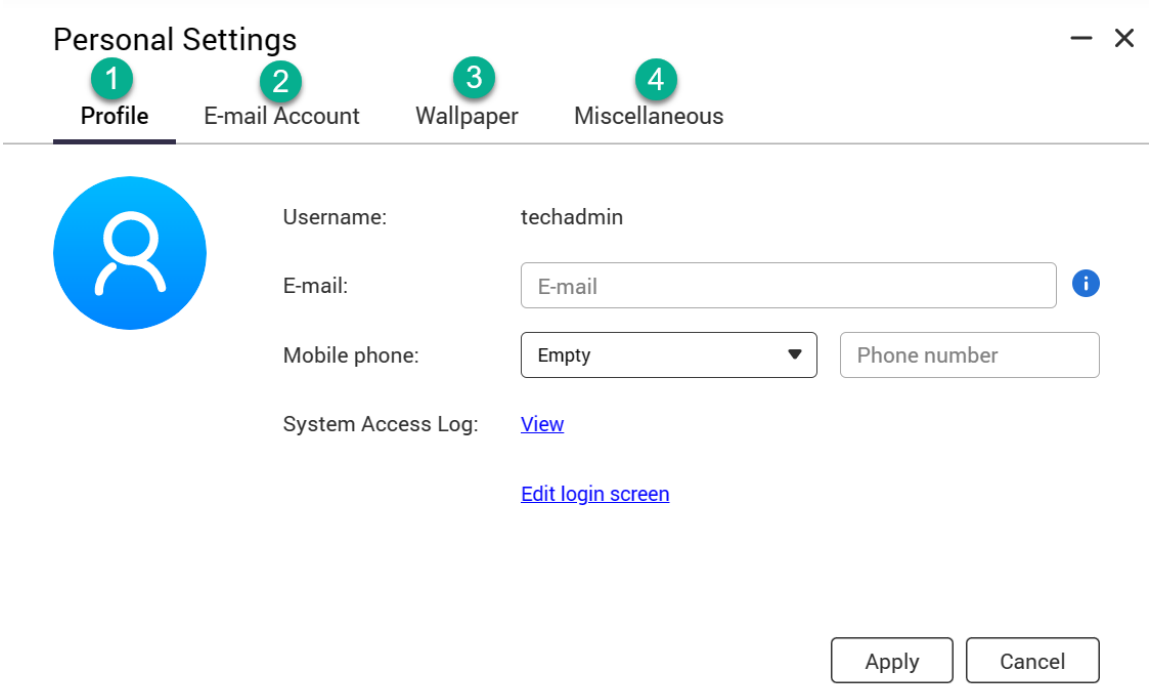
No.	Section	Displayed Information	User Actions
1	System Health	• NAS name • Uptime (number of days, hours, minutes and seconds) • Health status	Click the heading to open **Control Panel** > **System** > **System Status** > **System Information**. If disk-related issues occur, click the heading to open Storage Manager.
2	Hardware Information	• System temperature • System temperature • CPU fan speed • System fan speed	Click the heading to open **Control Panel** > **System** > **System Status** > **Hardware Information**.
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**.

No.	Section	Displayed Information	User Actions
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 Manager.
			• 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 Manager** > **Overview**.

No.	Section	Displayed Information	User Actions
6	Storage	For each shared folder: • Status • Used space • Available space • Folder size For each storage pool: • Status • Used space • Available space • Shared folder size For each LUN: • Status • Used space • Available space	• Click the heading to open the **Storage Resource** screen in the **Resource Monitor** window. • Click  to switch between shared folder and storage pool information.
7	Online Users	• Login time • Total connection time • Username • IP address • Client app • Connection type	Click the heading to open **Control Panel** > **System** > **QuLog Center** > **Online Users**.

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 QuTS Hero**: When enabled, QuTS hero 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, QuTS hero displays the desktop switching buttons **< >** on the left and right sides of the desktop.
		  • **Show the link bar on the desktop**: When enabled, QuTS hero displays the link bar on the bottom of the desktop.
		  • **Show the Dashboard button**: When enabled, QuTS hero displays the button to show the dashboard on the taskbar.
		  • **Show the NAS time on the desktop**: When enabled, QuTS hero displays the current NAS time, day, and date at the bottom-right of the desktop.
		  • **Keep Main Menu open after selection**: When enabled, QuTS hero 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, QuTS hero displays an **Autoplay** dialog box whenever an external storage device is inserted into a USB or SATA port.
		• Click **Apply** to save all changes.

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 Manager
		• 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 QuTS hero 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:
		• File Station
		• Helpdesk
		• License Center
		• Multimedia Console
		• Notification Center
		• QuTS hero SSL Certificate
			• Open a system utility or application in the QuTS hero 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 QuTS hero desktop. Users can either select from one of the provided wallpapers or upload an image.	Change the wallpaper in the **Options** window.

No.	Element	Description	Possible User Actions

2	Shortcut icons	Each icon opens an app or a utility.
		When you install an application, QuTS hero automatically creates a desktop shortcut. The following are the default shortcuts:
		• Control Panel
		• File Station
		• Storage Manager
		• 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	Date and time	This displays the date and time that the user configured during system installation.	N/A

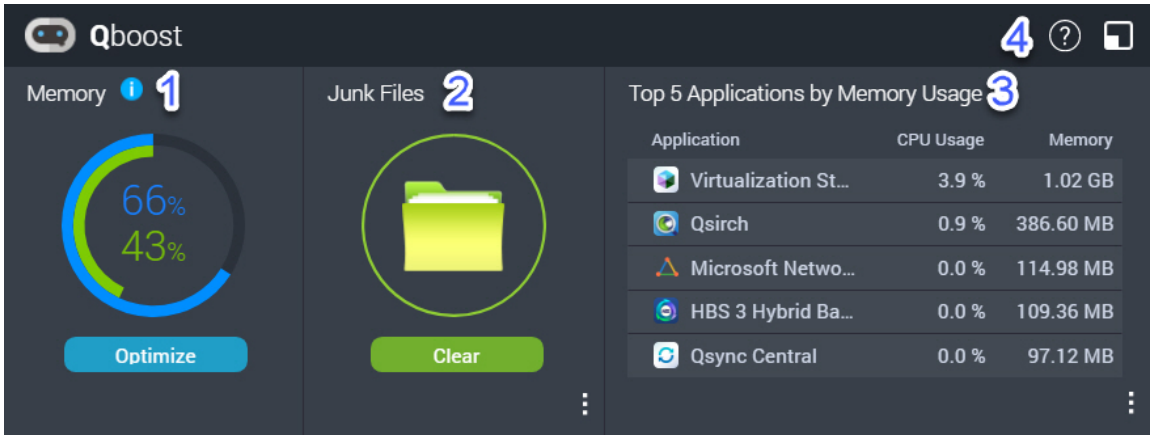
No.	Element	Description	Possible User Actions
5	Notifications	The system displays notifications in this area. Notifications inform the user of important system events that may require user action. If there are multiple notification groups, notices are arranged according to the notification type on a notice board. You can also view notifications in **Notice Board**. **Note** When you initialize QuTS hero, the Getting Started guide will appear in notifications after installation.	Click a notification to open the corresponding utility or app.
6	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

7	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

8	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.

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.

Login and Security

QNAP NAS provides a wide range of login options to help enhance your account and device security.

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

QuTS hero 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**.
   QuTS hero 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**.
    QuTS hero 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**.
   QuTS hero 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**.
    QuTS hero 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**.
    QuTS hero 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**.
   QuTS hero 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 QuTS hero also displays the same verification code.
14. On QNAP Authenticator, tap **Approve** if both verification codes match.
    QuTS hero 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**.
    QuTS hero 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**.
   QuTS hero 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**.
    QuTS hero 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**.
    QuTS hero displays a summary of your 2-step verification settings.

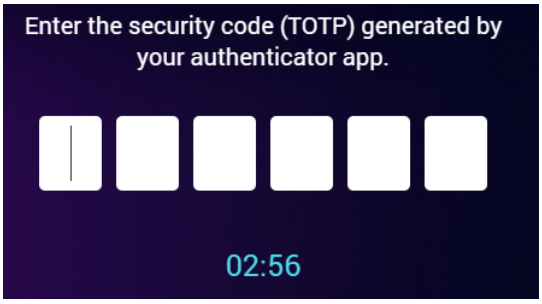
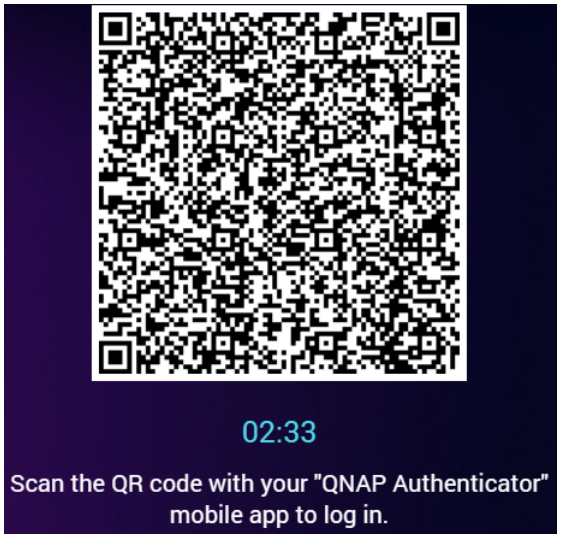
2-Step Verification is now enabled for your account. Starting from your next login, you will need to verify your identity with an online verification code (or with another method) after entering your password.

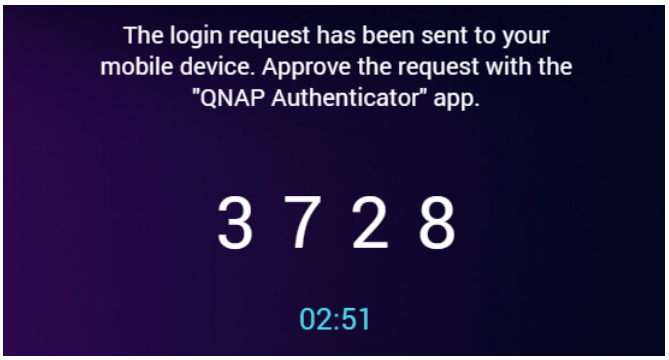
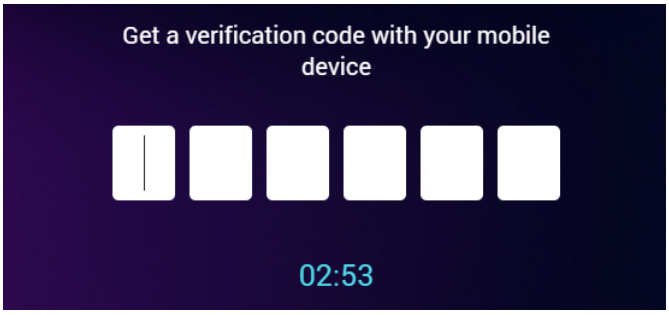
Logging in with 2-step verification

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 QuTS hero as administrator.
2. Go to **Control Panel** > **System** > **Security** > **2-step Verification**.
   QuTS hero 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

QuTS hero 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.

Verification Method	Description
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**.
   QuTS hero 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**.
    QuTS hero 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**.
   QuTS hero 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 QuTS hero 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**.
    QuTS hero displays a summary of your passwordless login settings.

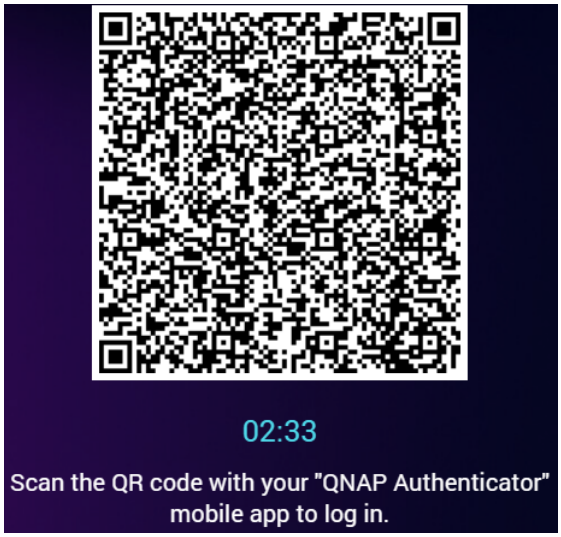
Passwordless login is now enabled for your account. Starting from your next login, you can verify your identity with a login approval without entering your password.

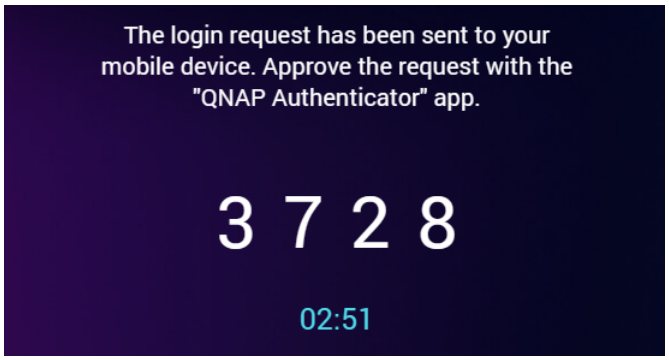
Logging in without your password

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. 

Verifi-cation 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.

Note
This topic explains how to disable passwordless login for your own account. If you are an administrator and and want to disable passwordless login for other users 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 **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.

Login with a QNAP ID

In addition to your NAS account, you can also choose to log in to the NAS with your QNAP ID. This allows you to streamline your device access.

Enabling NAS login via a QNAP ID

You can link your QNAP ID to your NAS account. This enables you to log in to the NAS directly with a QNAP ID to streamline your device access process.

Note

Before starting this task, ensure the following:

- The NAS administrator has enabled **Allow users to log in to this device with QNAP ID** in **Control Panel** > **System** > **Security** > **Login & Password**.
- You have set up 2-step verification for your NAS account.
- You have registered this NAS with your QNAP ID.

For more information, see 2-step verification and myQNAPcloud.

1. Go to **Desktop** > **Taskbar** > **[Username]** > **Login & Security** > **Advanced Settings**.
2. Under **Login with QNAP ID**, click **Link**.
   The login screen of the QNAP Account website appears.
3. Specify your QNAP ID and password.
4. Click **Sign in**.
5. Set up 2-step verification for your QNAP ID if you have not yet set it up. Click **Set Up Now**.

6. Select a verification method and follow the on-screen instructions to complete the setup.
   Once you have finished the setup, you will be automatically redirected back to the NAS. You will see your QNAP ID shown under **Login with QNAP ID**.

Now you can see the option **QNAP ID** on the NAS login screen. You can choose this option to log in with your QNAP ID. The QNAP Account website may require you to verify your identity with the verification method that you have chosen earlier.

Login with a Passkey

A passkey is a secure authentication method based on FIDO standards. With a passkey, you can log in to the NAS using the same mechanism that you use to unlock your computer, such as your fingerprint or PIN. A passkey is more secure than a traditional password and is more resistant to phishing attacks.

Enabling NAS login via a passkey

You can log in to the NAS with a passkey that follows the FIDO2 standard, which enables phising-resistant authentication methods that can further enhance your account and device security. This feature supports on-device authenticators such as Windows Hellow, Apple Touch ID, and PIN, and also external authenticators, such as a USB passkey. You can also use a passkey together with 2-step verification or passwordless login.

Note

Before starting this task, ensure that you have completed the following requirements:

- Install FIDO2 Server in the App Center.
- Set up an HTTPS connection and domain name for the NAS.

1. Go to **Desktop** > **Task Bar** > **[Username]** > **Login & Security** > **2-Step Verification or Passwordless Login**.
2. Enable **Passkey**.
3. Under **Manage devices**, go to the **Passkey** tab.
4. Click **Add**.
5. Enter your NAS password to verify your identity.
6. Follow the on-screen instructions to set up a passkey.

   Tip

   Depending on your operating system and your choice, you will see a wizard window that that requires you to specify your NAS credentials and verify your identity. For example, your device may ask you to scan your fingerprint.

7. Specify a name for your passkey.

8. Click **Finish**.
   Your passkey appears in the passkey list. You can add more passkeys or delete this passkey later.

The NAS login screen now displays the **Passkey** option. When you choose this option, you can verify your identity with your chosen method such as a fingerprint, a PIN, or a USB passkey.

High Availability

High Availability Manager is an application that enables you to create a high-availability (HA) environment for your system to enable continuous service in the event of hardware failures. The application allows you to create an HA cluster with two NAS devices, where the active node manages all data operations and services, while the passive node is a backup device that continuously synchronizes data and service settings from the active node. If the active node fails, the passive node will automatically take over to continue providing those services, ensuring uninterrupted business operations. Creating an HA cluster requires two identical NAS models running QuTS hero h5.3.0 or later, and High Availability Manager should be installed on both devices.

For details, see the following:

- High Availability Manager User Guide
- Frequently asked questions about high availability

Support and other resources

QNAP provides the following resources:

Resource	URL
Documentation	https://www.qnap.com/download
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/status
Downloads	https://www.qnap.com/download
QNAP Community	https://community.qnap.com
QNAP Accessories Store	https://accessory.qnap.com

2. Getting Started

After completing hardware setup and firmware installation, you can start creating storage pools and shared folders 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 and shared folders, which are features designed to help you facilitate data storage and management. You can configure storage settings in Storage Manager, a powerful built-in utility for storage management in QuTS hero.

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 shared folder.
   A shared folder is a storage space created from a storage pool, allowing you to divide and manage available storage capacity. QuTS hero provides several types of shared folders for different combinations of performance and flexibility. You need to create at least one shared folder to start storing data on the NAS.

   Tip
   A QuTS hero shared folder is the same as a QTS volume that contains one shared folder.

   For details, see Creating a shared folder.

Accessing data

QuTS hero 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 QuTS hero. 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 QuTS hero, 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 to back 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 data between your local NAS and multiple destinations, including a remote NAS, external devices, cloud storage services. You can also take snapshots for shared folders on your local NAS and use Snapshot Replica to back up these snapshots to another storage pool or 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. In addition to data deduplication and encryption, 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 shared folders.
  b. Back up snapshots with Snapshot Replica.

  An essential feature for data protection, a snapshot records the state of a shared folder at a specific point in time. Using a snapshot, you can restore a shared folder to a previous state or restore the previous versions of files. You can view and manage your snapshots in Snapshot Manager.

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 either on the source NAS or on the destination NAS.
For details, see:

- Taking a snapshot
- Creating a Snapshot Replica job

Configuring privilege settings

QuTS hero 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 QuTS hero. 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. Register the NAS to your QNAP ID.
   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 Setting up myQNAPcloud and AMIZ Cloud for the NAS.

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 theseQNAP applications on your mobile devices, you must sign in to them with your QNAP ID.
   For details, go to https://www.qnap.com/en/mobile-apps.

Acquiring apps and licenses

QuTS hero provides various essential applications to help manage your NAS. In addition to these built-in features, QuTS hero 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 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.

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 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.

2. Enable strong cipher suites.
3. Specify a port number.
4. Select **Force secure connection (HTTPS) only** to require all users to connect to the NAS using only HTTPS.

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

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

1. Click **Allowed Websites** to allow a specific website to embed QuTS hero in IFrames.
2. The **Allowed Websites** window appears.
3. Click **Add** to add a website to the list.
4. The **Add Host Name** window appears.
5. Specify a host name.
6. Click **Add**.
   The host name is added to the allowed websites list.

7. Select a website, and then click **Delete** to delete a website from the list.
8. 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.

Option	User Action
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**.
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**.

Action	Steps
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**.

Configuring console management

You can enable **Console Management** to peform basic configurations or maintenance tasks through the text-based software tool. This feature is disabled by default.

1. Go to **Control Panel** > **System** > **General Settings** > **Console Management**.
2. Select **Enable Console Management**.
3. 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. Optional: Click **Browse** to upload an intermediate certificate.

Option	User Action
Get from Let's Encrypt	**a.** Specify a domain name containing a maximum of 63 ASCII characters, without spaces. **b.** Optional: Specify a valid email address. **c.** 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**.
   QuTS hero 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: You can also choose to send a notification email to users a week in advance before their password expires.

4. Click **Apply**.

KMIP service

Enabling KMIP (Key Management Interoperability Protocol) service allows you to efficiently manage your encryption keys. By configuring a KMIP client and connecting it to a remote key server of your choice, you can store and access encryption keys in a single secure location. This allows you to streamline and centralize key management for certain NAS features, such as encrypted shared folders and encrypted LUNs.

Configuring KMIP client service

To enable KMIP client service on your device, you must first install KMIP Client in App Center, add a KMIP client certificate, and then connect to a KMIP server.

After enabling the KMIP client service, you can then enable saving encryption keys to the KMIP server in other applications.

1. Install KMIP Client.
   a. Log in to the system as an administrator.
   b. Open **App Center**, and then click  .
   A search box appears.
   c. Enter `KMIP Client`.
   KMIP Client appears in the search results.
   d. Click **Install**.
   The system installs KMIP Client.
2. Go to **Control Panel** > **System** > **Security** > **KMIP**.
3. Add a KMIP client certificate.
   a. Click **Add**.
   The **Add KMIP Client Certificate** window opens.
   b. Select one of the following:

Option	Description
Generate certificate	Automatically generate certificate files. **Note** If you select this option, you will need to import the certificate files to the KMIP server. 1. Click **Add**. The system automatically generates KMIP client certificate files. 2. Click **Download**. 3. Select the files to download. 4. Click **Download**. The system downloads the selected files to your computer. 5. Import the downloaded files to your KMIP server.

Option	Description
Import certificate	Import certificate files. **Note** If you are importing your own certificate files, use PEM files. 1. Next to **Certificate**, click **Browse** to upload the certificate file. 2. Next to **Private key**, click **Browse** to upload the private key file. 3. Optional: Next to **Intermediate certificate**, click **Browse** to upload the intermediate certificate file. 4. Click **Add**.

4. Configure the KMIP server connection.
   a. Click **Configuration Wizard**.
   The **KMIP Server Connection Settings** window opens.
   b. Specify the KMIP server's hostname or IP address.
   c. Specify the port number.
   The default port number is 5696.
   d. Optional: Specify a description.
   e. Click **Browse** to upload the certificate authority file.

      Note
      This step is required if you are using a self-signed certificate.

   f. Click **Connect**.
   The system connects to the KMIP server.
   The **Trust KMIP Server Certificate** window opens.
   g. Click **Trust**.
   The system saves the KMIP server connection settings.
   A confirmation message appears.
5. Click **OK** to enable the KMIP client.

The system enables the KMIP client.

Tip

- You can now enable storing encryption keys on the KMIP server for certain storage spaces such as encrypted shared folders and encrypted LUNs. Go to **Storage Manager** >  > **Storage** > **Store encryption keys on KMIP server**.
  After enabling this setting in Storage Manager, you can use the KMIP server to store encryption keys for your encrypted shared folders in Storage Manager, and for your encrypted LUNs in Storage Manager or iSCSI & Fibre Channel.
- To manage the KMIP client certificate, see Managing the KMIP client certificate.
- To manage the KMIP server connection or client service, see Managing the KMIP server connection and client service.

Managing the KMIP client certificate

1. Go to **Control Panel** > **System** > **Security** > **KMIP**.
2. Under **KMIP Client Certificate**, perform any of the following actions.

Action	Description
Add	Add a KMIP client certificate by generating or importing certificate files. For details, see Configuring KMIP client service.
Replace	Replace an existing KMIP client certificate. **Note** Replacing an existing KMIP client certificate may interrupt the KMIP server connection.
Download	Download existing KMIP client certificate files. **Note** If you generated the KMIP client certificate, you can download the certificate files and import them to your KMIP server.
Delete	Delete an existing KMIP client certificate. **Note** After deleting the certificate, you will need to add a certificate again the next time you try to connect to a KMIP server.

Managing the KMIP server connection and client service

1. Go to **Control Panel** > **System** > **Security** > **KMIP**.
2. Perform any of the following actions.

Action	User Action
Configure the KMIP server connection	Click **Configuration Wizard**. **Note** • This wizard helps you connect to a KMIP server. • You must add a KMIP client certificate before you can configure the KMIP server connection. • For details, see Configuring KMIP client service.
The following actions are only available after the KMIP server connection has been configured:	
Test the KMIP server connection	Under **KMIP Server Connection**, click **Test Connection**. **Note** The screen displays the date and time of the successful or failed connection attempt.
Edit the KMIP server connection settings	Under **KMIP Server Connection**, click **Edit**. **Note** You can only edit the KMIP server connection settings when the KMIP client service is enabled.
Clear the KMIP server connection settings	Under **KMIP Server Connection**, click **Clear**. **Important** • Clearing the KMIP server connection settings disables the KMIP client service. • After this action, the current device won't be able to access the encryption keys previously saved to the KMIP server.

Action	User Action
Enable the KMIP client service	Select **Enable KMIP client**. **Note** Enabling the KMIP client service allows certain applications to store encryption keys on the KMIP server.
Disable the KMIP client service	Deselect **Enable KMIP client**. **Note** If any applications are using the KMIP server to store encryption keys, you must first change the relevant settings in the applications before you can disable the KMIP client. **Important** After this action, the current device won't be able to access the encryption keys previously saved to the KMIP server.

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.

Settings	User Action
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. **Note** 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 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.
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.

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.

3. Click **Apply**.

Configuring the backup battery unit (BBU) settings

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

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

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

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

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

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.** QuTS hero monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. **b.** QuTS hero 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 QuTS hero 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 SR-IOV device settings.

Note
When the system is in a high-availability cluster, you can view information on expansion card resources installed on the passive node by selecting the passive node in the drop-down menu. However, you cannot configure any settings while viewing the passive node. Configurations saved in the active-node view will apply to both nodes.

1. Go to **Control Panel** > **System** > **Hardware** > **Hardware Resources**.
   QuTS hero 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
QuTS hero	QuTS hero applications share expansion card resources for transcoding. • Select **Hardware Transcoding** to allow QuTS hero 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

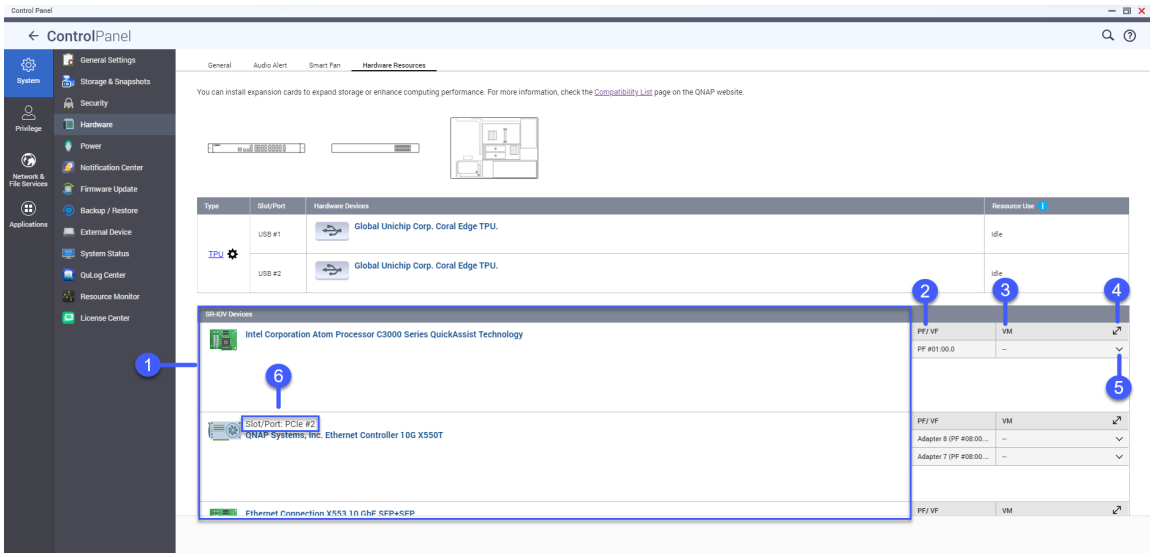
- The system will not run apps with lower TPU priority levels until the TPU resource is released from running higher priority apps.
- You can allocate up to four TPU devices to an app.

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 SR-IOV device 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	Hardware Devices	Lists all the SR-IOV devices that are mapped to your virtual machine (VM).
2	Physical Function/ Virtual Function	Displays the physical function (PF) or virtual function (VF) configured to the SR-IOV device.
3	Virtual Machine	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**.

Firmware update

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, QuTS hero 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 **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 automatic updates	You can configure QuTS hero to periodically download and install the latest firmware updates. For details, see Updating the firmware automatically.
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
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.
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.
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 updates	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 manually or using 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.
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 manually or using 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**.
   - QuTS hero checks for available firmware updates. You can choose to update QuTS hero 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. Optional: Click **Release notes** to view the release notes of the firmware update.
4. Optional: Select **Automatically restart the system if required for this update**.
5. Select the firmware update to download and install.

   Note
   For information on the types of available firmware updates, see , see Firmware 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.

Update/Notification Behavior	Description & Action
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.

   Tip
   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.
2. Download the device 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.

3. Go to **Control Panel** > **System** > **Firmware Update** > **Manual Installation**.
4. Click **Browse** and then select the extracted firmware package file.
5. Click **Update System**.
   A confirmation message window appears.
6. 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 QuTS hero.
- 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 QuTS hero 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

QuTS hero 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 QuTS hero, 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 QuTS hero 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.

   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 QuTS hero 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.

QuTS hero 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.
> - Shared folders on the current device that are not selected or that are not recorded in the system configuration file will be retained with their current configuration.

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

QuTS hero 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. 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, Basic system reset.
Advanced system reset	This performs a basic system reset and then restores the QuTS hero default settings, deleting all users and user groups. The user data stored on the disks is retained. For details, Advanced system reset.
Reinitialize the NAS	This deletes all data on the disks and reinstalls QuTS hero. For details, 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

Setting	Default Values
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 QuTS hero 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.

Method	Steps
Using QuTS hero	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.

Reinitializing the NAS

Reinitializing the NAS deletes all data on the disks and reinstalls QuTS hero.

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**.

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.

Phase	Scenario	NAS Behavior
Phase 2: From the end of the specified waiting time until the UPS runs out of power	The power is restored, and the NAS is powered off.	The NAS remains powered off.
Phase 3: From the moment the UPS runs out power until the power is restored	The power is not restored, and the NAS is in auto-protection mode.	The NAS powers off.
	The power is not restored, and the NAS is powered off.	The NAS remains powered off.
	The power is restored.	The NAS applies the specified power recovery settings.

Configuring 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 QuTS hero 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.

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 QuTS hero. • 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**.

Section	Description
Overview	This screen provides a general summary of CPU usage, memory usage, network usage, and ongoing processes on the NAS.

Section	Description
System Resource	This screen uses line charts to display CPU usage, memory usage, network usage, and graphics card usage (if supported and installed) over time. You can hover the mouse pointer over a line chart to view the hardware usage at a specific point in time. **Tip** You can click **More** (⋮) and then select **Settings** to specify the time interval on the line charts.
Storage Resource	This screen uses line charts to display the activities of volumes, LUNs, storage pools, RAID groups, and disks on the NAS over time. This screen also summarizes the storage usage of each volume. You can hover the mouse pointer over a line chart to view the storage activity at a specific point in time.
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 QuTS hero. **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 QuTS hero. 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, QuTS hero 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 this device. For details, see SMS notifications. **Note** Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
Email (optional)	Specify an email address that will receive notifications from this device. 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	An UID will be generated automatically for the user. **Note** Users can change the UID. Click  to specify a custom UID.

Field	Description
Send a notification mail to the newly created user (optional)	When selected, this device sends a message to the specified email address that contains the following information: • Username and password • URLs for connecting to the NAS **Tip** Users have the option to edit the notification message. To edit the notification message, follow these steps: **a.** Click **Edit Message**. The **Edit Message** window appears. **b.** Specify a subject and message. **c.** Click **Save**. **d.** Optional: To use the default message, click **Restore to Defaults**.

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.
By default, administrator accounts have access to all applications.

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.

> **Important**
> Individual quotas may override group quotas.

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** QuTS hero removes leading zeros in starting numbers. For example, `001` becomes `1`.

Field	Description
Number of Users	Specify the number of users (1–4095). Example: `5`
Password	Specify a password that contains a maximum of 64 ASCII characters.
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, QuTS hero 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**.
   QuTS hero creates the user accounts and adds them to the displayed user list.
8. 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, QuTS hero sends a message that contains the following information to the specified email address of the user. • Username and password • URLs for connecting to the NAS **Important** To send email notifications, ensure that you have configured an SMTP server. For details, see Configuring an email notification server.
Overwrite duplicate users	When selected, QuTS hero overwrites existing user accounts that have duplicates on the imported user account list.
User must change the password at first logon	When selected, the imported user must change the password when logging in for the first time. The password may contain a maximum of 64 ASCII characters.

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

Important
Ensure that you are importing a valid QuTS hero 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**.
   QuTS hero 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**.
   QuTS hero 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 QuTS hero.

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: • **Description (optional)**: Specify a user description that contains a maximum of 50 characters. • **Disallow the user to change password**: When selected, the operating system 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. • **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. **d.** Optional: Click **Disable 2-step Verification**. **Note** For details, see Disabling 2-step verification. **e.** Click **OK**.

Task	User Action
Edit user group	**a.** Under **Action**, click  . The **Edit User Group** window appears. **b.** Select or deselect user groups. **c.** Click **Apply**.
Edit shared folder permission	**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. Click **OK**.

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 storage pool.
   Home folders are stored on the selected storage pool.
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

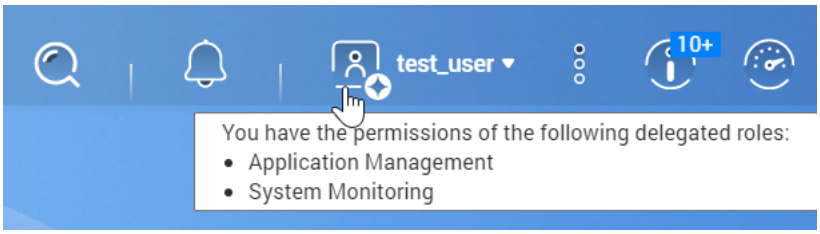
Delegated Administration allows administrators to assign one or more pre-defined roles to non-administrator users or groups. With delegated roles, non-administrator users can help manage system resources and perform routine tasks, such as updating apps, monitoring CPU usage, and backing up important 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 Manager, Snapshot Manager, 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 App Center.	• Unable to manually install apps or configure settings in 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 QuTS hero 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, QuTS hero 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, QuTS hero 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 QuTS hero 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, QuTS hero 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 QuTS hero 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 QuTS hero as administrator.
2. Go to **Control Panel** > **Privilege** > **Delegated Administration**.
3. Click **Permission Viewer**.
4. Click **Export**.

QuTS hero 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 QuTS hero 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**.

QuTS hero 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

QuTS hero 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**.

QuTS hero restores the default shared folders.

Creating a shared folder

> **Note**
> For shared folders created in QuTS hero h5.0.1 and later, read acceleration is enabled by default and cannot be disabled.
> For details, see "Enable Read Acceleration" in Shared folder management.

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Shared Folder**.
2. Click **Create**, and then select **Shared Folder**.
   The **Create Shared Folder** wizard opens.
3. Specify a shared folder name.
   - The name can be in any Unicode language.
   - The maximum length is 64 bytes. In English, this equals 64 characters.
   - The following special characters are not allowed: @ " + = / \ : | * ? < > ; [ ] % , ` ' non-breaking space
   - The last character cannot be a period (.) or space.
   - The name cannot begin with a space or "_sn_".
4. Optional: Specify a description.
   The information is for your reference and is not used by QuTS hero.
5. Select a storage pool.
   The shared folder is created using storage space from this pool.
6. Select a method of space allocation.

Allocation	Description
Thick provisioning	QuTS hero allocates storage pool space when the shared folder is created, ensuring the space is available.

Allocation	Description
Thin provisioning	QuTS hero allocates storage pool space on demand, as data is written to the shared folder. **Note** This option is selected by default.

7. Specify the capacity of the shared folder.
The method of space allocation determines the maximum shared folder capacity.

Method	Maximum Size
Thick provisioning	Less than the amount of free space in the parent storage pool. Some space is reserved for the system.
Thin provisioning	5 PB (5000 TB) **Tip** • Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation. • If you do not specify the folder quota, it will be equal to the storage pool quota.

Note
If the parent storage pool does not contain any existing shared folders, setting the allocated quota to maximum may cause the storage pool size to exceed the pool space alert threshold. If this happens, the pool space alert will be disabled.
To reset the pool space alert, see Configuring storage pool space alerts.

8. Optional: Configure shared folder guaranteed snapshot space.
Shared folder guaranteed snapshot space is storage pool space that is reserved for storing snapshots of a folder. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots for this folder.

Note
This setting is only available for thick shared folders.

9. Click **Advanced Settings**.

10. Optional: Configure shared folder encryption.

    Note

    - To encrypt data on the shared folder, the system generates a unique encryption key based on the user-defined encryption password. To access data on the shared folder, the shared folder must be unlocked with the encryption password, the encryption key file, or via a KMIP server. You can download the encryption key file later.
    - You cannot enable or disable encryption after a shared folder is created.
    - Encryption decreases read and write speeds.

    a. Next to **Storage Settings**, click  .

    b. Next to **Folder Encryption**, click  .

    c. Specify an encryption password.
    The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed.

    Warning
    If you forget the encryption password and do not have the encryption key file, the shared folder will become inaccessible and all data in the shared folder will be lost. To download the encryption key file, see Managing shared folder encryption.

    d. Verify the password.

    e. Optional: Enable **Auto unlock on startup**.

    Note

    - This setting allows the system to save the encryption key so it can automatically unlock the shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
    - By default, the system stores the encryption key on the NAS and unlocks with this key. If you enabled storing encryption keys on a KMIP server, you can choose to store the encryption key on the KMIP server in the next step.
    - You can change this setting at any time. For details, see Managing shared folder encryption.

f. Optional: Select an auto unlock option.

> **Note**
> This step is only available when all of the following are true:
>
> - You enabled **Auto unlock on startup**.
> - You enabled KMIP service.
>   For details, see KMIP service.
> - You enabled storing encryption keys on the KMIP server.
>   For details, see Storage global settings.

- **Unlock with encryption key stored on NAS** (default): This option stores the encryption key on the NAS.
- **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server.

11. Optional: Configure WORM (Write Once Read Many).
WORM prevents anyone from modifying or deleting files or folders in the shared folder.

> **Important**
> This setting cannot be modified after shared folder creation.

a. Next to **Security Settings**, click .

b. Next to **WORM**, click .

c. Configure any of the following settings.

Setting	Description
Mode	Select a WORM mode. • **Enterprise** Users can delete the shared folder. • **Compliance** Users cannot delete the shared folder. An administrator must remove the storage pool to delete the WORM shared folder. **Note** You cannot modify the WORM mode after folder creation.

Setting	Description
Lock setting	Configure whether files in the shared folder are to be locked automatically or manually. If you choose to lock files automatically, specify the amount of time to delay locking the file after the file is added to the folder. After this time has passed, the file becomes unmodifiable. If you choose to lock files manually, after a file is added to the folder, you can manually configure the file permissions to read-only at any time. **Note** • You cannot modify the lock setting after folder creation. • The time a file becomes locked might vary from the specified time by +/- 1 minute. • The maximum lock delay time is 168 hours and 59 minutes.
Set retention period	Limit how long WORM applies to each file and folder. Files and folders can be deleted after the specified time period.

12. Optional: Next to **Storage Settings**, click to configure any of the following settings.

Setting	Description
Compression	QuTS hero compresses the data in the shared folder to reduce the size of stored data. Enabling compression also reduces the total number of blocks that QuTS hero needs to read and write, increasing read and write speeds. **Tip** Compression does not impact read/write and processor performance on ZFS file systems. Only disable this setting when necessary.
Deduplication	QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data. **Important** To enable deduplication, your NAS must have at least 16 GB of memory.

Setting	Description
SSD read cache	QuTS hero adds data from this folder to the SSD cache to improve read performance. **Important** Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.
Fast clone	Fast Clone enables QuTS hero to create copies of files faster. It also saves storage space by modifying file metadata, allowing original and copied files to share the same data blocks. **Important** • To enable this setting, **Thin provision** must be selected. • Fast Clone only works when the copied file is created in the shared folder containing the original file. • Fast Clone does not improve the speed of snapshot restoration operations such as restoring files from a snapshot, snapshot revert, and snapshot clone.
ZIL synchronized I/O mode	Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes: • **Auto**: QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • **Always**: All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a small impact on performance. • **None**: 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.

Setting	Description
Performance profile (block size)	Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application. **Tip** The default is 128K.
Target tier	**Note** This setting is only available when the shared folder is in a Qtier hero storage pool. This setting determines the primary tier in which the shared folder's data is stored. Select a tier based on how frequently the data is accessed: • **High-speed tier** Uses PCIe/NVMe SSDs for the fastest read/write performance. Ideal for frequently accessed data. • **Medium-speed tier** Uses SAS/SATA SSDs for balancing performance and capacity. Suitable for daily operations. • **Low-speed tier** Uses SAS/SATA HDDs for long-term storage. Ideal for infrequently accessed data.

Setting	Description
Write acceleration mode	**Note** • This setting is only available when the shared folder is in a Qtier hero storage pool. • This setting is unavailable when the high-speed tier is selected as the target tier, in which case the system automatically writes data directly to the high-speed tier and stores the data there. This setting determines how data reaches the target tier depending on your read/write needs. • **Write-buffer** Data is first written to the fastest tier and then moved to the target tier. This mode is ideal for I/O-intensive applications where you want to fully leverage the speed of SSDs for write operations. • **Load-balance** Data is written to the fastest tier and the target tier simultaneously, reducing load on any single tier. This mode is suitable for frequently writing large volumes of data but where read operations are infrequent, such as continuous log archiving. • **Direct-write** Data is written directly to the target tier, bypassing the fastest tier (no acceleration). This mode is ideal for situations where both read and write operations are not very frequent, such as creating backups or archiving old data.

13. Click **Review and Create**.
14. Review the summary information.
15. Click **Create**.

QuTS hero creates the shared folder.

If you enabled encryption and selected **Unlock with encryption key stored on KMIP server**, the system automatically stores the encryption key on the KMIP server.

You can configure shared folder permissions in Control Panel. For details, see Shared folder permissions.

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.

Option	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : | * ? < > ; [ ] % `.
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters. The information is for your reference and is not used by QuTS hero.
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 and the kernel-mode SMB daemon is disabled. 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.

Option	Description
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **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.
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.

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, QuTS hero 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.

Note
HybridMount shared folders can only modify **Comment (optional)**, **Enable access-based share enumeration (ABSE)**, **Enable access-based enumeration (ABE)**, and **Set this folder as the Time Machine backup folder (macOS)**.

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.
   - A shared folder with WORM enabled can only be removed if the WORM type is **Enterprise**.

3. Click **Remove**.
   A confirmation message appears.
4. Click **Yes**.

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.

Mounting an ISO file as a shared folder

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

5. Specify the following information.

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

6. Click **Next**.
7. Configure user access permissions and guest access rights to the ISO shared folder.

Type	Option	Description	User Action
User access permissions	**Grant read-only access right for adminis-trators 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.

Type	Option	Description	User Action
User access permissions	**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**.
   QuTS hero 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

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. Click on any of the following tabs:
   - **Users and groups permission**
   - **NFS host access**
   - **Microsoft Networking host access**

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.** Optional: Select **Individual permissions**. **Note** You can't select this for folders mounted by HybridMount using SMD and NFS file protocols. These folders do not support Access-control list (ACL) permission settings. You will also not be able to expand subfolders created through SMB and NFS file protocols. When selected, you can apply protocol-specific settings. **1.** Configuring for RW shared folders and RO subfolders: **a.** Select **Read/Write** permission for each user. **b.** Click to delete the user group **Everyone**. **c.** Click **Apply**. **d.** Select a shared folder, and change permission style to **Windows Special Permissions**. **e.** Select one or more permission inheritance policies. • Replace all file and subfolder permissions with inherited permissions from this folder • Disable inheritance and remove all inherited permissions from this folder (this option is only available to subfolders) • Disable inheritance and convert inherited permissions on this folder into explicit permissions (this option is only available to subfolders)

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.	**f.** Click and select permissions for the user. **Tip** You can choose to only apply these permissions to files and subfolders within this folder. **g.** Click **OK**. **h.** Optional: Add users or groups to the list of users with permissions for the shared folder. 1. Click **Add Users**. The **Add Users and Groups** window appears. 2. Select or search a user or user group. 3. Click to edit the user or user group's permissions, then click **OK**. 4. Optional: Edit more users or user groups. 5. Click **OK**. QuTS hero adds the users and their corresponding permissions to the list. **2.** Configuring for RO shared folders and RW subfolders: **a.** Select **Read/Write** permission for each user. **b.** Go to ACL permission, specify a user, and click **Read Only**. **c.** Click to delete the user group **Everyone**. **d.** Click **Apply**. **e.** Add a user and select **Read/Write**.

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.	f. Click **Apply**. b. Optional: Remove a user from the list of users with permissions for the shared folder. 1. Locate the user you want to remove. 2. Click  . QuTS hero removes the user from the list.
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. Optional: Select any of the following options: • **sync** Select a sync option for this setting. • **secure** c. Under **Host / IP / Network**, enter an IP address or domain name. d. Optional: Add an NFS host. Under **Allowed IP Address or Domain Name**, click **Add**. QuTS hero adds an entry to the list. e. Optional: Delete an NFS host. 1. Select an NFS host from the list. 2. Click **Delete**.

Permission Type	Description	User Action
Microsoft Networking host access	Specify which computers can access shared folders through Microsoft Networking.	**a.** Add a Microsoft Networking host. **1.** Click **Add**. QuTS hero 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**.

Conflicts in shared folder permissions

When a user is assigned different permissions for a shared folder, QuTS hero 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

User Permission	User Group Permission	Actual Permission
Read Only	Read/Write	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 create up to 50 portal folders, and you can link up to 10 folders to a single portal folder.

Starting with QuTS hero h6.0.x, the folder aggregation feature has been moved to the SMB Service application. To enable it, open SMB Service, go to **SMB Service** > **Folder Aggregation**, and select **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. Open SMB Service.
2. Go to **SMB Service** > **Folder Aggregation**.

3. Click **Create**.
   The **Create a Portal Folder** window appears.
4. 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.
	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.

5. Enable **Users must login before accessing the portal folder** to ensure that only authenticated users can access the portal folder, blocking guest access and unauthorized connections.
6. Click **Apply**.

SMB Service creates a portal folder.

Modifying portal folder information

> **Note**
> Ensure that folder aggregation is enabled before performing the following steps. For details, see Folder aggregation.

1. Open SMB Service.
2. Go to **SMB Service** > **Folder Aggregation**.
3. Locate a portal folder.

4. Perform any of the following tasks.

Task	User Action
Edit portal folder properties	a. Under **Action**, click  . The **Edit Portal Folder** window appears. b. Edit the folder properties. For details, see Creating a portal folder.
Configure the remote folder link	a. Under **Action**, click  . The **Remote Folder Link** window appears. b. Double-click the **Name**, **Host Name**, and **Remote Shared Folder** fields to specify the information for the remote folder link. c. Click **Apply**.

5. Click **Apply**.

SMB Service saves the modified portal folder settings.

Deleting portal folders

> **Note**
> Ensure that folder aggregation is enabled before performing the following steps. For details, see Folder aggregation.

1. Open SMB Service.
2. Go to **SMB Service** > **Folder Aggregation**.
3. Select the portal folders that you want to delete.
4. Click **Delete**.
   A warning message appears.
5. Click **OK**.

SMB Service deletes the selected portal folders.

Importing folder trees

> **Note**
> Ensure that folder aggregation is enabled before performing the following steps. For details, see Folder aggregation.

1. Open SMB Service.

2. Go to **SMB Service** > **Folder Aggregation**.
3. Click **Import Folder Tree**.
   The **Import Folder Tree** window appears.
4. Click **Browse**.
5. Select the file that contains the folder tree.

   Important
   Ensure that you are importing a valid QuTS hero folder tree file to avoid parsing errors.

6. Click **Open**.
   The File Explorer window closes.
7. Click **Apply**.
   QuTS hero imports the folder tree and closes the import window.
8. Click **Apply**.

SMB Service imports the folder tree.

Exporting folder trees

Note
Ensure that folder aggregation is enabled before performing the following steps. For details, see Folder aggregation.

1. Open SMB Service.
2. Go to **SMB Service** > **Folder Aggregation**.
3. Click **Export Folder Tree**.
   QuTS hero 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 QuTS hero.

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.

You can only encrypt shared folders when creating them. For details, see Creating a 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, QuTS hero 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**.

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**. QuTS hero 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, QuTS hero automatically unlocks the shared folder after the NAS restarts. **c.** Enter the encryption password. **d.** Click **OK**. QuTS hero 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**. QuTS hero 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.

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.

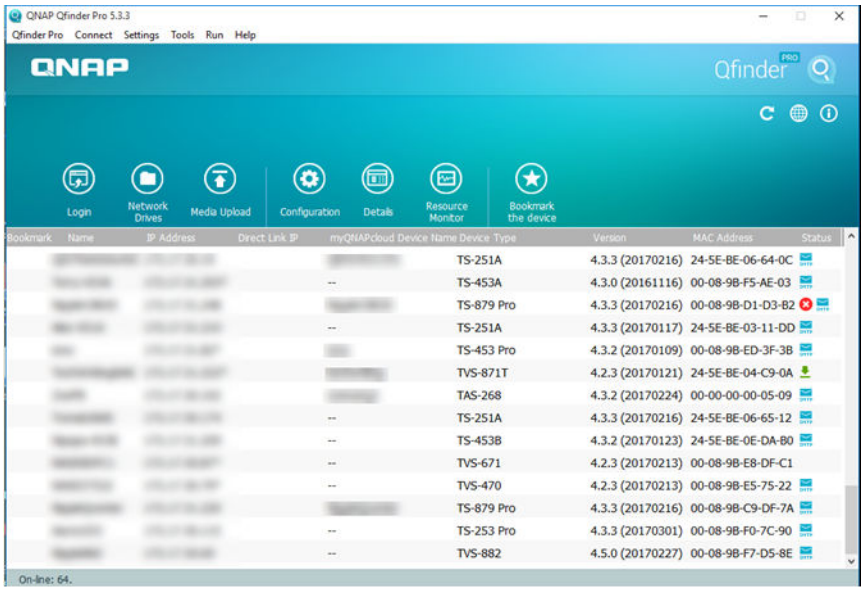
For Windows and Mac, you can use Qfinder Pro to map or mount your NAS shared folders. Qfinder Pro is a desktop utility that enables you to locate and access the QNAP NAS devices in your local area network.

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

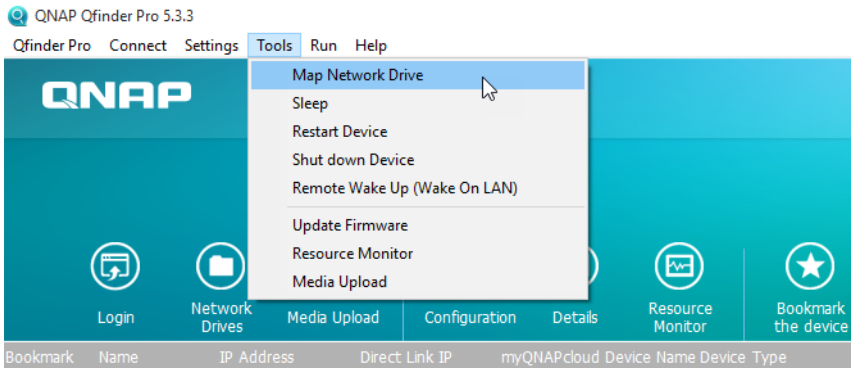
Mapping a shared folder on a Windows computer

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.

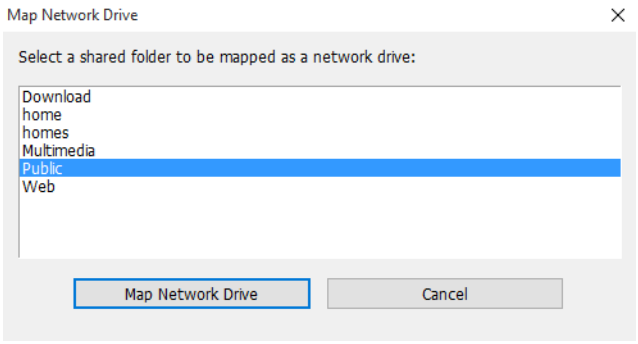


4. Select the NAS where the shared folder is located.
5. Click **Tools** > **Map Network Drive**.

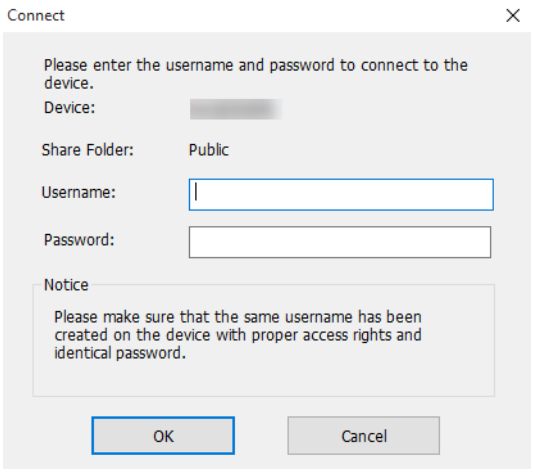


6. Select a shared folder.

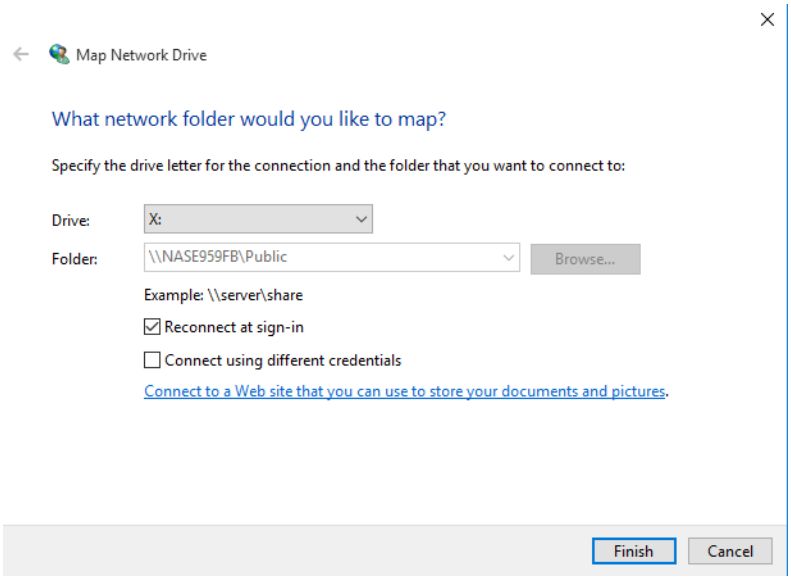
7. Click **Map Network Drive**.



8. Specify your QuTS hero 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.
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**.

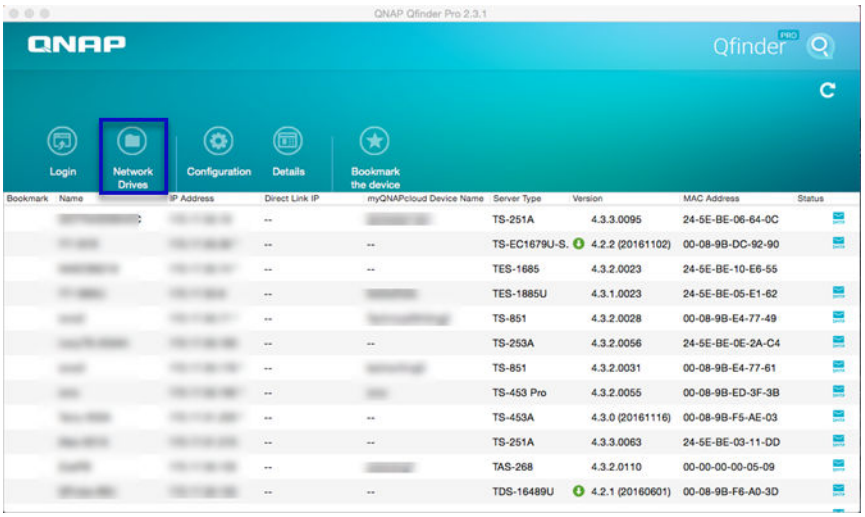
The shared folder is mapped as a network drive and can be accessed using Windows Explorer.

Mounting a shared folder on a Mac computer

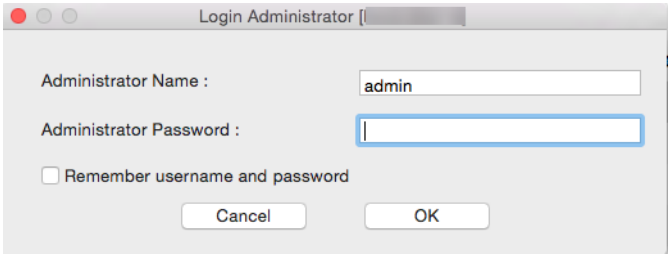
Before mounting a shared folder, ensure that you have Qfinder Pro installed on your Mac computer.

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**.

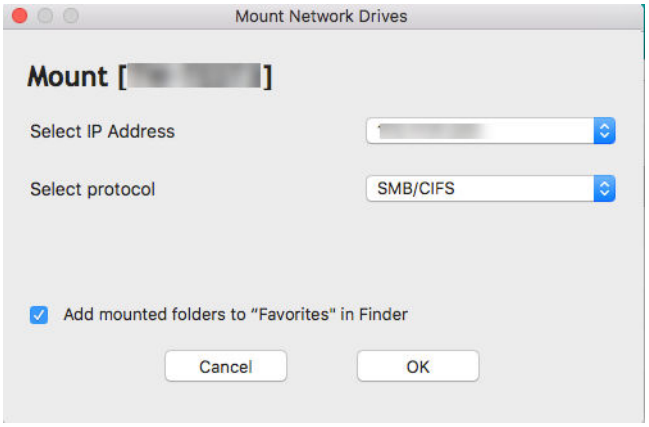


6. Specify your QuTS hero username and password.
7. Click **OK**.



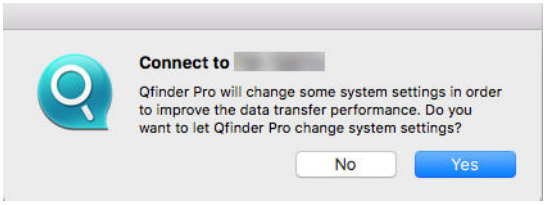
The **Mount Network Drives** window opens.

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

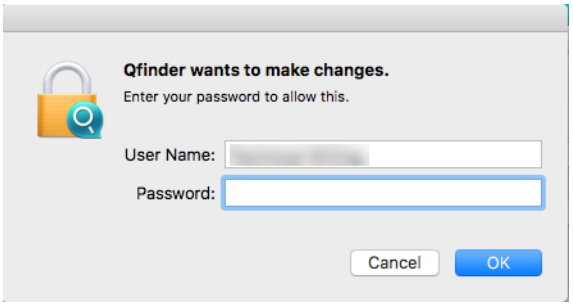


A confirmation message appears.

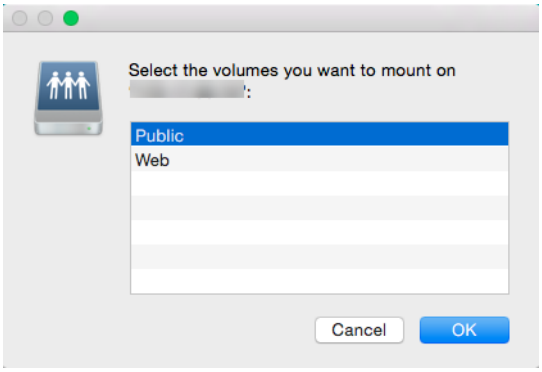
10. Click **Yes**.



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, QuTS hero prevents users from saving data to the NAS after the quota is reached. By default, quotas are not enabled for users.

QuTS hero 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.
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 shared folder and are not shared across shared folders.

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**.
   QuTS hero 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**.

QuTS hero exports the quota settings as a CSV file.

Quota conflicts

QuTS hero 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
QuTS hero 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.
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 Domain Services (AD DS), commonly referred to as Active Directory (AD), is a Microsoft directory service that stores and manages information about users, groups, and computers within a domain. It provides centralized authentication and authorization using LDAP and Kerberos protocols in Windows environments.

When a NAS joins an AD domain, it becomes a member of that domain and communicates with the domain controller (DC) to authenticate users. The NAS retrieves and caches user and group

information from the AD domain as needed. AD users can then sign in to the NAS using their existing domain credentials.

Configuring AD authentication using the Quick Configuration Wizard

1. Go to **Control Panel** > **Privilege** > **Domain Security** > **Windows AD/LDAP**.
2. Enable **AD authentication (domain members)**.
3. Click **Quick Configuration Wizard**.
   The **Active Directory Wizard** appears.
4. Click **Next**.
5. Specify the fully domain name of the AD DNS server.
   QuTS hero 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 to secure message transmissions and prevent relay attacks.
    - **Sign if client agrees**: The server signs SMB messages only if the client also supports and requests signing. This provides basic protection while maintaining compatibility with older clients.
    - **Enforce signing**: The server requires all SMB message transmissions to be signed. Clients that do not support signing will be denied access. This ensures maximum security against relay and tampering attacks.
    - **Sign according to selected SMB version**: The server applies message signing rules based on the configured SMB protocol version. Signing behavior follows the version-specific security policies (for example, SMB 3.0 and later always enforce signing).
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** > **Windows AD/LDAP**.
2. Enable **AD authentication (domain members)**.
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**
   - **Add NAS to 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 to secure message transmissions and prevent relay attacks.
   - **Sign if client agrees**: The server signs SMB messages only if the client also supports and requests signing. This provides basic protection while maintaining compatibility with older clients.
   - **Enforce signing**: The server requires all SMB message transmissions to be signed. Clients that do not support signing will be denied access. This ensures maximum security against relay and tampering attacks.
   - **Sign according to selected SMB version**: The server applies message signing rules based on the configured SMB protocol version. Signing behavior follows the version-specific security policies (for example, SMB 3.0 and later always enforce signing).
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 DS 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 DS. You can only enable trusted domains on the NAS. By default, this feature is disabled in QuTS hero.

Note

To enable trusted domains, you must first enable and configure AD authentication. For details, see the following.

- Configuring AD authentication using the Quick Configuration Wizard
- Configuring AD authentication manually

1. Open SMB Service.
   The **Overview** page appears.
2. Go to **SMB Service** > **Settings** > **General**.
3. Enable **SMB Service**.
4. Click **Apply**.
5. Click **Advanced**.
6. Scroll down to the **Additional Settings** section.
7. Select **Enable trusted domains** to allow users from trusted external domains to access the NAS using their domain credentials.

   Note
   This setting is only available if the NAS is joined to an AD DS domain.
8. Click **Apply**.

SMB Service enables trusted domain authentication/

Microsoft Entra 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
Microsoft Entra ID was formerly named Azure Active Directory (Azure AD). The updated name aligns with Microsoft's broader Entra platform for identity and access management. For details, see New name for Azure Active Directory.

Enabling Microsoft Entra single sign-on (SSO)

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.
- To register an application in the Microsoft Entra admin center and then configure SSO settings on the NAS, see How can I configure Microsoft Entra Domain Services single sign-on for a QNAP NAS?
- 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 Microsoft Entra single sign-on (SSO)**.
3. Specify the **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 the **Tenant ID**.
   For details, visit https://learn.microsoft.com/entra/fundamentals/how-to-find-tenant.
5. Click **Apply**.

   Note

   Your NAS login screen changes to include a Microsoft Entra 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 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.
	Search scope	Select a search scope option to specify how deeply the NAS searches the directory tree when querying the remote LDAP server. • **One-level**: Searches only the immediate child entries under the base DN. • **Subtree**: Searches the base DN and all entries within its subdirectories.

LDAP Server Type	Fields	User Action
Remote LDAP server	**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:	
	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**.
   QuTS hero 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.

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

Tip

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

5. Click **Apply**.

Managing AD and LDAP user groups

1. Go to **Control Panel** > **Privilege** > **User Groups**.
2. Select **Domain Groups**.
   QuTS hero 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. QuTS hero 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

Note

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

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

Important

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

3. Select the domain controller mode.

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

4. Specify the following information.

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

5. 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** > **Applications** > **Domain Controller**.
2. Click **Reset**.
   A dialog box appears.
3. Enter the administrator password.
4. Click **OK**.

Default domain user accounts

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

Creating a domain user

1. Go to **Control Panel** > **Applications** > **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: " + = / \ : | * ? < > ; [ ] % `'

Field	Description
Password	Specify a password between 8 and 127 characters that contains at least three of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
Verify Password	Verify the domain user password.
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 QuTS hero. 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** > **Applications** > **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** QuTS hero removes leading zeros in starting numbers. For example, `001` becomes `1`.
Number of Users	Specify a number between 1 and 4095. This number signifies the number of accounts that will be created.
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**.
   QuTS hero 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** > **Applications** > **Domain Controller** > **Users**.
2. Click **Create** > **Batch Import Users**.
   The **Batch Import Users** wizard appears.
3. Optional: Select **Overwrite existing users**.

Important
When selected, QuTS hero 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 QuTS hero 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**.
   QuTS hero imports the domain user account list.
7. Click **Finish**.

Modifying domain user account information

1. Go to **Control Panel** > **Applications** > **Domain Controller** > **Users**.
2. Locate a user.
3. Perform any of the following tasks.

Task	User Action
Change password	**a.** Under **Action**, go to ⋮ > **Edit password**. 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**, go to ⋮ > **Edit user properties**. 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**, go to ⋮ > **Edit group membership**. 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**, go to ⋮ > **Edit user profile**. 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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **Domain Controller** > **Computers**.
2. Locate a computer account.
3. Perform any of the following tasks.

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

4. Click **Finish**.

Deleting computer accounts

1. Go to **Control Panel** > **Applications** > **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** > **Applications** > **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.
Move a value down	a. Select a value from the list. b. Click  . The value moves down in the list.

Task	User Action
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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **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** > **Applications** > **Domain Controller** > **Backup/Restore**.
2. Under **Back up ADDC Database**, enable **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** > **Applications** > **Domain Controller** > **Backup/Restore**.
2. Under **Restore ADDC Database**, click **Browse**.
3. Locate a domain controller backup file.
4. Click **Import**.

5. Services

QuTS hero 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 QuTS hero 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**.

QuTS hero enables antivirus.

Scanning shared folders

1. Log on to QuTS hero 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	QuTS hero only reports detected viruses and does not take any further action. The detections will appear in **Reports**.
Move infected files to quarantine	QuTS hero 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	QuTS hero 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 QuTS hero 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 . QuTS hero starts the scan job.
Edit	a. Select . The **Details** window opens. b. Modify the settings. c. Click **OK**. QuTS hero 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**. QuTS hero deletes the scan job.

Managing reported scan jobs

1. Log on to QuTS hero 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 . QuTS hero 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**. QuTS hero deletes the scan job.

Managing quarantined files

Warning
You cannot recover deleted quarantined files.

1. Log on to QuTS hero 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  . QuTS hero 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  . QuTS hero 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  . QuTS hero 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 QuTS hero 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**.

    QuTS hero 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 QuTS hero 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**.

   QuTS hero 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**.

   QuTS hero saves the changes.

6. Optional: Restore a php.ini file.

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

   b. Click **OK**.

   QuTS hero 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 QuTS hero 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 storage pool.

Enabling the LDAP server

1. Log on to QuTS hero 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 QuTS hero 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 QuTS hero 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**.

QuTS hero 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. QuTS hero 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 QuTS hero.

MariaDB server requirements

Software requirements	Description
Operating system	QuTS hero 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 QuTS hero 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 QuTS hero 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**.
   QuTS hero 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**.
    QuTS hero enables the MariaDB server.

Restoring a MariaDB database

1. Log on to QuTS hero 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**.
   QuTS hero 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**.
   QuTS hero 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 QuTS hero 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**.
   QuTS hero 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**.
   QuTS hero enables the MariaDB server.

Enabling or disabling the MariaDB server

> **Important**
> On devices with QuTS hero 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 QuTS hero 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 QuTS hero 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 QuTS hero 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 QuTS hero 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 QuTS hero 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**.
   QuTS hero adds the syslog filter.

Managing syslog filters

1. Log on to QuTS hero 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.
   QuTS hero enables the syslog filter.
5. Click to disable the filter.
   QuTS hero disables the syslog filter.
6. Modify the syslog filter.
   a. Click .
      The **Filter** window opens.
   b. Modify the filter.
   c. Click **Apply**.

   QuTS hero 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**.

   QuTS hero 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 QuTS hero 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 QuTS hero 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**.
   QuTS hero creates the RADIUS client.

Managing RADIUS clients

1. Log on to QuTS hero 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.
   QuTS hero enables the client.
5. Click to disable the client.
   QuTS hero disables the client.
6. Edit the client information.
   a. Click .
      The **Edit Client** window opens.
   b. Configure the client information.
   c. Click **Apply**.

   QuTS hero 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**.

   QuTS hero 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 QuTS hero 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**.
   QuTS hero creates the RADIUS user.

Managing RADIUS users

1. Log on to QuTS hero 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.
   QuTS hero enables the user.
5. Click to disable the user.
   QuTS hero disables the user.
6. Change the RADIUS user password.
   a. Click .
      The **Edit User** window opens.
   b. Modify the settings.
   c. Click **Apply**.

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

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

c. Click **Yes**.

QuTS hero 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 QuTS hero 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**.
   QuTS hero 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 QuTS hero 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**.
   QuTS hero enables the NTP server.

6. File Station

About File Station

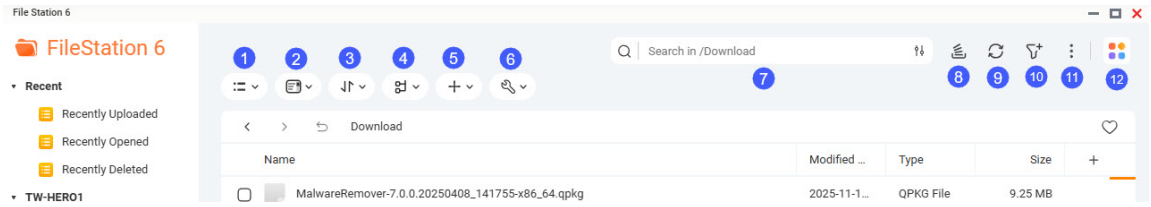
File Station is a QuTS hero file management application that allows you to access files on the NAS. You can quickly locate files and folders, manage access permissions, play media files, and share data with other users.

System requirements

Category	Detail
Web browser	• Microsoft Edge • Mozilla Firefox 3.6 or later • Apple Safari 5 or later • Google Chrome

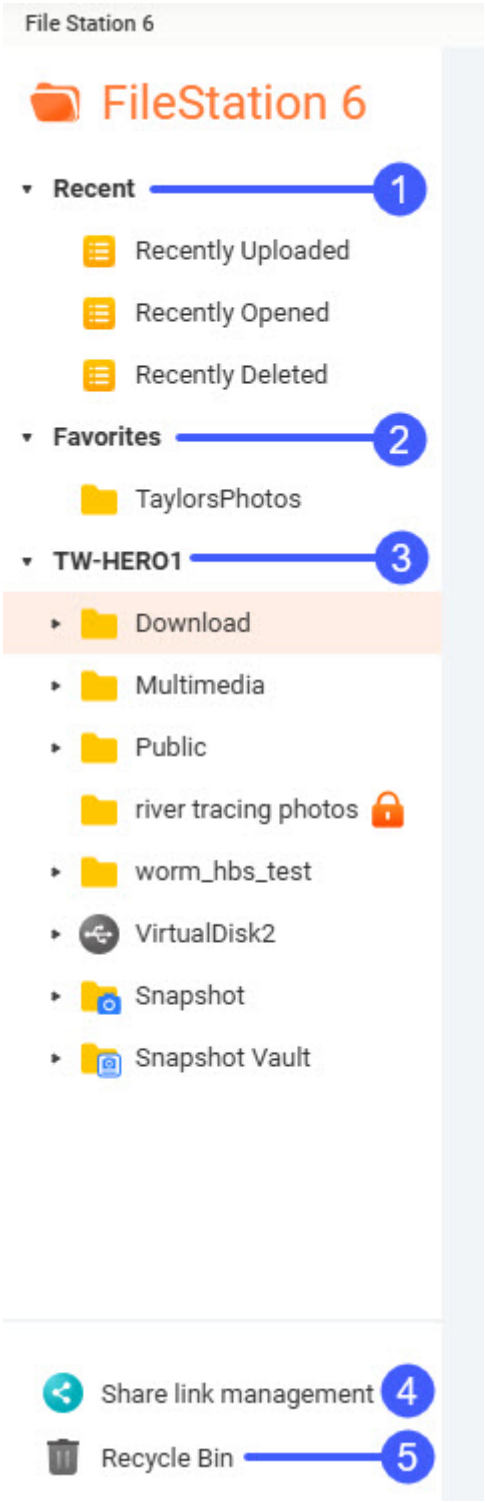
File Station user interface

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



Label	Item	Description
1	View mode	Select a view mode
2	Display mode	Select a display mode.
3	Sort	Sort current items.
4	Group by	Group current items. **Note** This button is not available when **Page mode** is selected for the view mode.

Label	Item	Description
5	New item	Create a new folders, upload new files and folders, and create other types of items.
6	More actions	Perform different tasks. **Note** Some task options only appear when you select certain types of files.
7	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.
8	Background Task	Open the background tasks of your mount, folder, or file operations.
9	Refresh	Refresh the current page.
10	Smart Filter	Filter files and folders based on the specified criteria.
11	More settings	Configure File Station settings, open the Help guide, or view application information.
12	More apps	View details of other file management apps. Click an app name to view the app in App Center. **Tip** View this menu frequently for details on the latest file management apps from QNAP.



Label	UI Element	Description
1	Recent	Displays recently uploaded, opened, or deleted files.
3	Favorites	Displays bookmarked folders.

Label	UI Element	Description
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	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.
WebDAV	Displays a list of connections mounted through a local network or over the internet.
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.

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.

Category	File Extension
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.
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	

Operation	File Tasks	Folder Tasks
Access	• Downloading files and folders • Viewing file or folder properties	
	• 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 • Locking or unlocking an encrypted shared folder
Play	• Playing an audio file • Playing a video file • Playing a video file using CAYIN Media Viewer • Opening a 360-degree image or video file	-
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 **Upload File** or **Upload Folder**. Select the files or folders you want to upload and then click **Open** or **Upload**.

   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
Enable **Set this as the default action, and do not ask me again.** to 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 size of the selected files or folders.
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.
Volume	Displays the name of the volume on which the folder is stored.

4. Click **Close**.

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**.
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** > **Open with Chrome Extension**.
Using the context menu	Right-click the file and then select **Open with** > **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** > **Open with Text Editor**.
Using the context menu	**a.** Right-click the file. **b.** Select **Open with** > **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 **Open with** > **View in Google docs**.
Using the context menu	Right-click and then select **Open with** > **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 **Open with** > **Edit with Office Online**.
Using the context menu	Right-click the file and then select **Open with** > **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** > **Open with Image2PDF**.
Use the context menu	Right-click and then select **Open with** > **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 a list of Qsync folders.

3. Click one of the following Qsync folders:

Qsync Folder	Description
Synced Files	Files synced with other devices via Qsync Central.
Accepted Team Folder	Folders shared by other NAS users that you have accepted.
Backups	Backups taken by Qsync Central.

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**.
3. Click the **Share Link** tab.
   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.

4. 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  .

Task	User Action
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 **Share link management**.
3. Click the **Shared with me** tab.

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

1. Open File Station.
2. Click  .
   The **Sort By** menu opens.
3. For the first input box, select one the following:
   - Name
   - Modified Date
   - Type
   - Size
   - Permission

   File Station sorts files and folders according to the selected option.
4. For the second input box, select **Ascending** or **Descending**.
   File Station sorts files and folders in an ascending or descending order.

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**.
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**.

Method	Steps
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**.
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.** Right-click inside the folder and then select **Paste**.

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**.

Method	Steps
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**.
	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**.

Method	Steps
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**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Compress**.

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

Option	Task
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.

Option	Description
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**.
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 Recycle Bin
   - Delete permanently

   Note

   - If the file is in a shared folder with WORM enabled, the file can be permanently deleted only if the WORM type is set to **Enterprise** and only after the specified retention period.
   - WORM files cannot be moved to the Recycle Bin.

5. Click **OK**.
   File Station either moves the selected file to the Recycle Bin or deletes it permanently.

Restoring a deleted file

1. Open File Station.

2. Go to **Recycle Bin**.
   The Recycle Bin opens and displays recycle locations.
3. Click a recycle location to open it.
4. Locate the file.
5. 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.
6. 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**.

Method	Steps
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 **Create 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 **New** > **Create folder**. The **Create folder** window opens. 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**.

Method	Steps
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

1. If you have not yet configured a default system email, then configure a default system email first.
   a. Go to the system desktop.
   b. In the upper right corner, click  .
   The **Personal Settings** window appears.
   c. Click the **Email Account** tab.
   d. Click **+ Add**.
   The **Setup E-mail Account** window opens.
   e. Enter the required information.
   f. At the bottom of the **Setup E-mail Account** window, enable **Set as default account.**.
   g. Click **Finish**.
2. Open File Station.
3. Locate the file or folder.
4. Perform one of the following methods.

Method	User Action
Using the toolbar	**a.** Select the file or folder. **b.** Click  . **c.** Select **Share** > **Via Email**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** > **Via Email**.

The **Share** window appears.

5. 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.

6. 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**.

7. 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 **Share** > **To Social Network**.
Using the context menu	a. Right-click the file or folder. b. Select **Share** > **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 **Share** > **Create share link only**.

Method	User Action
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** > **Create share link only** .

The **Share** window appears with the **Create share link only** tab selected..

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 Media Viewer from App Center and activate a CAYIN Media Viewer 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 **Share 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 **Share** > **To NAS user**.

Method	User Action
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** > **To NAS user**.

The **Share** window appears with the **NAS user** tab open..

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

Note
For shared folders created in QuTS hero h5.0.1 and later, read acceleration is enabled by default and cannot be disabled.
For details, see "Enable Read Acceleration" in Shared folder management.

1. Open File Station.
2. On the menu bar, click  .
3. Select **Create a Shared Folder**.
   The **Create Shared Folder** wizard opens.
4. Specify a shared folder name.
   - The name can be in any Unicode language.
   - The maximum length is 64 bytes. In English, this equals 64 characters.
   - The following special characters are not allowed: @ " + = / \ : | * ? < > ; [ ] % , ` ' non-breaking space
   - The last character cannot be a period (.) or space.
   - The name cannot begin with a space or "_sn_".

5. Optional: Specify a description.
   The information is for your reference and is not used by QuTS hero.
6. Select a storage pool.
   The shared folder is created using storage space from this pool.
7. Select a method of space allocation.

Allocation	Description
Thick provisioning	QuTS hero allocates storage pool space when the shared folder is created, ensuring the space is available.
Thin provisioning	QuTS hero allocates storage pool space on demand, as data is written to the shared folder. **Note** This option is selected by default.

8. Specify the capacity of the shared folder.
   The method of space allocation determines the maximum shared folder capacity.

Method	Maximum Size
Thick provisioning	Less than the amount of free space in the parent storage pool. Some space is reserved for the system.
Thin provisioning	5 PB (5000 TB) **Tip** • Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation. • If you do not specify the folder quota, it will be equal to the storage pool quota.

Note
If the parent storage pool does not contain any existing shared folders, setting the allocated quota to maximum may cause the storage pool size to exceed the pool space alert threshold. If this happens, the pool space alert will be disabled.
To reset the pool space alert, see Configuring storage pool space alerts.

9. Optional: Configure shared folder guaranteed snapshot space.
   Shared folder guaranteed snapshot space is storage pool space that is reserved for storing snapshots of a folder. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots for this folder.

   Note
   This setting is only available for thick shared folders.

10. Click **Advanced Settings**.
11. Optional: Configure shared folder encryption.

    Note

    - To encrypt data on the shared folder, the system generates a unique encryption key based on the user-defined encryption password. To access data on the shared folder, the shared folder must be unlocked with the encryption password, the encryption key file, or via a KMIP server. You can download the encryption key file later.
    - You cannot enable or disable encryption after a shared folder is created.
    - Encryption decreases read and write speeds.

    a. Next to **Storage Settings**, click  .

    b. Next to **Folder Encryption**, click  .

    c. Specify an encryption password.
       The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed.

       Warning
       If you forget the encryption password and do not have the encryption key file, the shared folder will become inaccessible and all data in the shared folder will be lost. To download the encryption key file, see Managing shared folder encryption.

    d. Verify the password.

e. Optional: Enable **Auto unlock on startup**.

> **Note**
>
> - This setting allows the system to save the encryption key so it can automatically unlock the shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
> - By default, the system stores the encryption key on the NAS and unlocks with this key. If you enabled storing encryption keys on a KMIP server, you can choose to store the encryption key on the KMIP server in the next step.
> - You can change this setting at any time. For details, see Managing shared folder encryption.

f. Optional: Select an auto unlock option.

> **Note**
>
> This step is only available when all of the following are true:
>
> - You enabled **Auto unlock on startup**.
> - You enabled KMIP service.
>   For details, see KMIP service.
> - You enabled storing encryption keys on the KMIP server.
>   For details, see Storage global settings.

- **Unlock with encryption key stored on NAS** (default): This option stores the encryption key on the NAS.
- **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server.

12. Optional: Configure WORM (Write Once Read Many).
WORM prevents anyone from modifying or deleting files or folders in the shared folder.

> **Important**
>
> This setting cannot be modified after shared folder creation.

a. Next to **Security Settings**, click .

b. Next to **WORM**, click .

c. Configure any of the following settings.

Setting	Description
Mode	Select a WORM mode. • **Enterprise** Users can delete the shared folder. • **Compliance** Users cannot delete the shared folder. An administrator must remove the storage pool to delete the WORM shared folder. **Note** You cannot modify the WORM mode after folder creation.
Lock setting	Configure whether files in the shared folder are to be locked automatically or manually. If you choose to lock files automatically, specify the amount of time to delay locking the file after the file is added to the folder. After this time has passed, the file becomes unmodifiable. If you choose to lock files manually, after a file is added to the folder, you can manually configure the file permissions to read-only at any time. **Note** • You cannot modify the lock setting after folder creation. • The time a file becomes locked might vary from the specified time by +/- 1 minute. • The maximum lock delay time is 168 hours and 59 minutes.
Set retention period	Limit how long WORM applies to each file and folder. Files and folders can be deleted after the specified time period.

13. Optional: Next to **Storage Settings**, click to configure any of the following settings.

Setting	Description
Compression	QuTS hero compresses the data in the shared folder to reduce the size of stored data. Enabling compression also reduces the total number of blocks that QuTS hero needs to read and write, increasing read and write speeds. **Tip** Compression does not impact read/write and processor performance on ZFS file systems. Only disable this setting when necessary.
Deduplication	QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data. **Important** To enable deduplication, your NAS must have at least 16 GB of memory.
SSD read cache	QuTS hero adds data from this folder to the SSD cache to improve read performance. **Important** Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.
Fast clone	Fast Clone enables QuTS hero to create copies of files faster. It also saves storage space by modifying file metadata, allowing original and copied files to share the same data blocks. **Important** • To enable this setting, **Thin provision** must be selected. • Fast Clone only works when the copied file is created in the shared folder containing the original file. • Fast Clone does not improve the speed of snapshot restoration operations such as restoring files from a snapshot, snapshot revert, and snapshot clone.

Setting	Description
ZIL synchronized I/O mode	Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes: • **Auto**: QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • **Always**: All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a small impact on performance. • **None**: 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.
Performance profile (block size)	Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application. **Tip** The default is 128K.
Target tier	**Note** This setting is only available when the shared folder is in a Qtier hero storage pool. This setting determines the primary tier in which the shared folder's data is stored. Select a tier based on how frequently the data is accessed: • **High-speed tier** Uses PCIe/NVMe SSDs for the fastest read/write performance. Ideal for frequently accessed data. • **Medium-speed tier** Uses SAS/SATA SSDs for balancing performance and capacity. Suitable for daily operations. • **Low-speed tier** Uses SAS/SATA HDDs for long-term storage. Ideal for infrequently accessed data.

Setting	Description
Write acceleration mode	**Note** • This setting is only available when the shared folder is in a Qtier hero storage pool. • This setting is unavailable when the high-speed tier is selected as the target tier, in which case the system automatically writes data directly to the high-speed tier and stores the data there. This setting determines how data reaches the target tier depending on your read/write needs. • **Write-buffer** Data is first written to the fastest tier and then moved to the target tier. This mode is ideal for I/O-intensive applications where you want to fully leverage the speed of SSDs for write operations. • **Load-balance** Data is written to the fastest tier and the target tier simultaneously, reducing load on any single tier. This mode is suitable for frequently writing large volumes of data but where read operations are infrequent, such as continuous log archiving. • **Direct-write** Data is written directly to the target tier, bypassing the fastest tier (no acceleration). This mode is ideal for situations where both read and write operations are not very frequent, such as creating backups or archiving old data.

14. Click **Review and Create**.
15. Review the summary information.
16. Click **Create**.

QuTS hero creates the shared folder.

If you enabled encryption and selected **Unlock with encryption key stored on KMIP server**, the system automatically stores the encryption key on the KMIP server.

You can configure shared folder permissions in Control Panel. For details, see Shared folder permissions.

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 Viewer 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. **Note** Certain resolutions may require Video Station, CAYIN Media Viewer and a CAYIN Media Viewer license.

Method	Steps
Using the context menu	**a.** Right-click the file. **b.** Select **Play**. **c.** Select a resolution. **Note** Certain resolutions may require Video Station, CAYIN Media Viewer and a CAYIN Media Viewer license.

File Station plays the selected file using Media Viewer.

Playing a video file using CAYIN Media Viewer

CAYIN Media Viewer is a third-party multimedia application that can be installed from App Center. A CAYIN Media Viewer license is required to play videos with CAYIN Media Viewer however many common video formats can be played with a free CAYIN Media Viewer license available from the QNAP Software Store.

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** > **Play with CAYIN Media Viewer**.
Using the context menu	**a.** Right-click the file. **b.** Click **Play** > **Play with CAYIN Media Viewer**

File Station plays the selected file using CAYIN Media Viewer.

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**.

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**.

Method	Steps
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.

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 Media Viewer fromApp Center and activate a CAYIN Media Viewer 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**.

Method	Steps
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.
	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/tutorial/con_show.php?cid=479.

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**.

Method	Steps
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**.

Viewing file properties

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 **Properties**.
Using the context menu	**a.** Right-click the file. **b.** Select **Properties**.

The **Properties** window opens and displays the following information.

Field	Description
Selected Items	Displays the number of selected items.
Type	Displays the file type.
Size	Displays the file size.
File Path	Displays the folder location.
Modified Date	Displays the date that the file was last modified.
Owner	Displays name of the NAS user who uploaded the file.
Group	Displays the name of the NAS group that can access the file.

Field	Description
Storage Pool	Displays the name of the storage pool on which the file is located.
View Access Logs	Keeps track of access to the file. **Tip** You can view access logs in QuLog Center. **a.** Open QuLog Center. **b.** Go to **Local Device** > **System Access Logs**. **c.** Specify File Station in the search field.

4. Click **Close**.

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 Qsirch mode 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
Keyword	Searches by file or folder name. **Note** In Qsirch mode, File Station additionally searches inside the text contents of files for matching keywords.
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.

Field	Description
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 Qsirch mode to search for file content

Searching with Qsirch mode active 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 **Qsirch** toggle button at the top of the drop-down search box.
4. Specify at least one of the following fields.

Field	Description
Keyword	Searches by file or folder name. Additionally searches inside the text contents of files for matching keywords.
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**.

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.
Allow all users to share files via "Share > To NAS User" and send share notifications through email	File Station allows non-administrators to share 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.

Option	Description
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, then enable and configure thumbnail generation services in Multimedia Console.

Option	Description
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. Under **Display thumbnails for documents** configure document thumbnail options.

   Important
   This feature requires Qsirch. You can install it from the App Center.

   a. In the first selection box, select a document thumbnail option.

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.

Option	Description
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)

b. In the second selection box, select the document types that File Station will generate thumbnails for.

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 Manager

> **Note**
> This utility is only accessible to administrators and users with the System Management role.

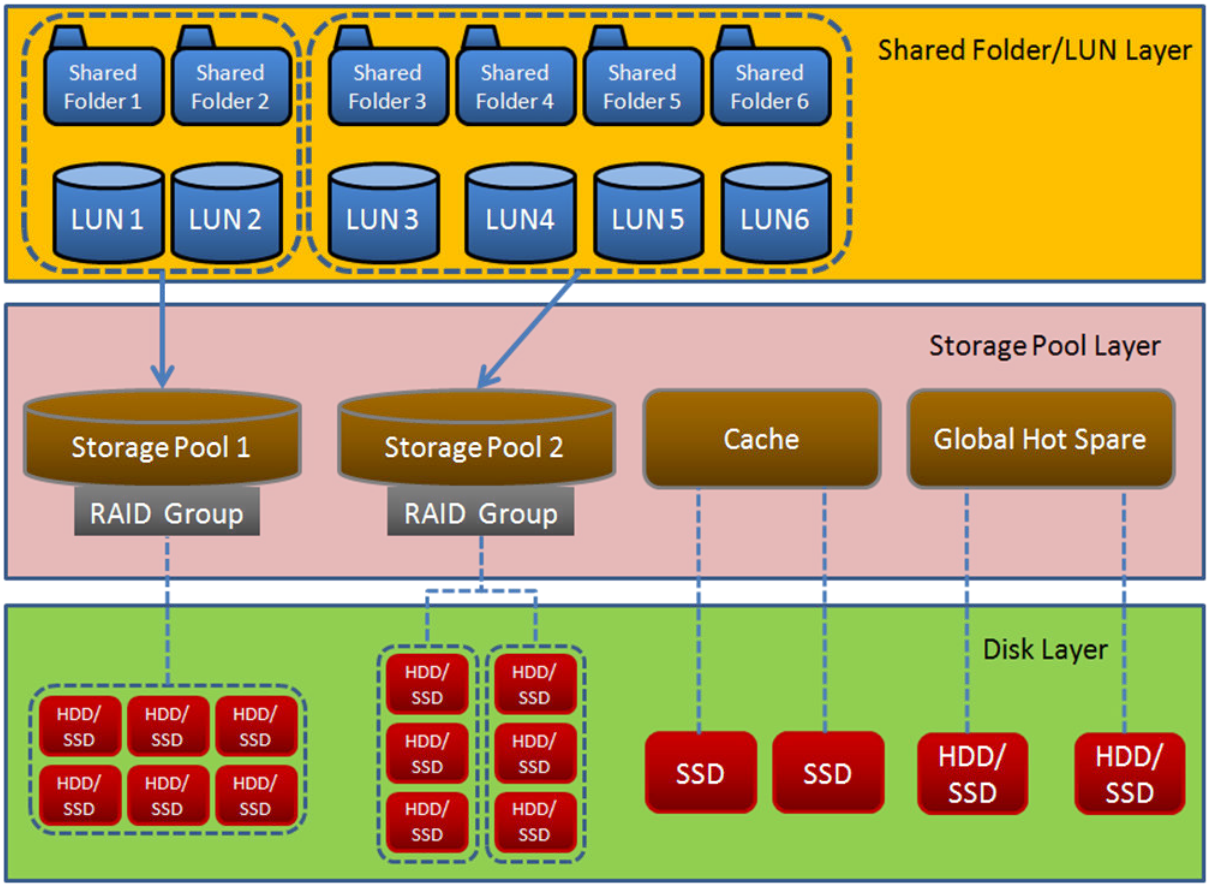
Storage Manager is a QuTS hero utility that helps you create, manage, and monitor storage on your NAS. With Storage Manager you can perform the following tasks:

- Create RAID groups, storage pools, and shared folders.
- Monitor storage usage and access speeds.
- Accelerate the performance of your NAS by creating an SSD cache.
- Manage external storage devices.
- Create local virtual disks and storage pools from remote storage space.

QNAP flexible storage architecture

QNAP flexible storage architecture consists of three layers, which combine to offer storage flexibility and data protection.

- Disks
- Storage pools
- Shared folders and LUNs (logical unit numbers)



Tip

You can expand the storage capacity of your NAS by connecting a QNAP expansion unit. For details on compatible models, see www.qnap.com/compatibility or your NAS hardware user guide.

Global settings

You can access global settings by clicking in the Storage Manager window.

Storage global settings

You can configure storage global settings in **Storage Manager** > > **Storage**.

Setting	Description
Pool scrubbing schedule	Pool scrubbing detects and automatically repairs damaged data blocks in the ZFS file system. **Important** The scrubbing task may reduce the storage pool read and write performance. You should schedule pool scrubbing to run during times of low NAS usage. You can also click **Exclude Times** to specify times and days of the week during which scrubbing will not run.
Clean Deduplication Table	When ZFS performs deduplication, it records duplicate data in a deduplication table. Cleaning removes unused entries from the deduplication table. **Important** The clean deduplication table task may reduce the system read and write performance. You should schedule this task to run during times of low NAS usage.
ARC RAM Usage	ZFS uses Adaptive Replacement Cache (ARC), an algorithm which uses as much RAM as possible to optimize system performance. Lowering the maximum ARC RAM usage can provide applications with more access to RAM, but may affect ZFS performance. **Warning** Increasing the maximum ARC RAM usage can cause currently running applications to close. Review your NAS RAM usage before you proceed. **Note** This setting is disabled if the total NAS RAM size is 8 GB, in which case the minimum and maximum ARC RAM usage must be the same.
Store encryption keys on KMIP server	Enable this feature to allow the system to store encryption keys on the KMIP server for encrypted shared folders and encrypted LUNs. **Note** To enable to feature, KMIP Client must be installed in App Center, and the KMIP client must be enabled in **Control Panel** > **System** > **Security** > **KMIP**. For details, see KMIP service.

Disk health global settings

You can configure disk health global settings in **Storage Manager** >  > **Disk Health**.

Setting	Description
Predictive Migration	Enable this feature to regularly monitor disk health and allow QuTS hero to automatically replace a disk before it fails. If any of the specified events occur, QuTS hero displays a warning and then begins migrating data from the faulty disk to a spare disk. After the migration is finished, the healthy disk is used in place of the faulty disk. This process is safer than manually initiating a full RAID rebuild after a disk has failed.
S.M.A.R.T. polling time	Specify how often QuTS hero checks disks for S.M.A.R.T. errors in minutes.
Disk Temperature Alarm	Enable this feature to monitor the disk temperatures. QuTS hero 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.
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. QuTS hero 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 QuTS hero 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, QuTS hero uses the default TLER/ERC settings specified by the disk manufacturer.

Setting	Description
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.

Storage

QuTS hero provides a flexible storage architecture that enables you to easily manage, store, and share files.

Disks

Disk types

QuTS hero restricts which types of disks can be used to create an SSD cache or storage pool.

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.
- 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 QuTS hero.

Disk Type	Installation Method	SSD Cache	Storage Pools
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

Disk Type	Installation Method	SSD Cache	Storage Pools
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 • NAS drive bay (some NAS models only)	Yes	No

Note
QuTS hero supports Seagate dual-actuator HDDs. In Storage Manager, these disks are labeled with the tag `Seagate DA`.

Disk management

You can manage disks in **Storage Manager** > **Disks**. Select a disk to view its status and hardware details.

Disk statuses and usage types

Disk health status

You can view the health status of a disk in the following locations:

- **Storage Manager** > **Disks** > **Device**, in the left panel and in the **Summary** tab
- **Storage Manager** > **Disks** > **Disk**, under the **Status** column

Status	Description
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.

Disk behavioral status

You can view the behavioral status of a disk in **Storage Manager** > **Disks** > **Device**, in the **Summary** tab, under **Status**.

Status	Description
Ready	`Ready`: The disk is ready.

Status	Description
Migrating	`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.

Disk usage type

You can view the usage type of a disk in the following locations:

- **Storage Manager** > **Disks** > **Device**, in the left panel
- **Storage Manager** > **Disks** > **Disk**, under the **Usage Type** column

Usage Type	Description
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.

Disk information

To view information on a disk, go to **Storage Manager** > **Disks** > **Device**, and then select the disk. Storage Manager displays the location of the disk on the NAS and various information in dedicated tabs.

Tab	Description
Summary	Displays general information about the disk, such as status, manufacturer, model, disk capacity, and more.

Tab	Description
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 storage pool. 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.
SSD Features	Displays features pertaining to solid-state drives.
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 QuTS hero, the SMART attribute's status changes to `Warning`.

Disk actions

Action	User Action
Detach	Go to **Storage Manager** > **Disks** > **Device**, select a disk, and then 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 Manager** > **Disks** > **Device**, select a disk, and then click **Action** > **Disable Spare**. Unassigns the disk as a global hot spare.

Action	User Action
Locate	Go to **Storage Manager** > **Disks** > **Device**, select a disk, and then 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 Manager** > **Disks** > **Device**, and then click ⋮ > **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 Manager** > **Disks** > **Device**, select a disk, and then 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 set as the new spare disk or safely detached from the RAID group and the system.
Scan for bad blocks	Go to **Storage Manager** > **Disks** > **Device**, select a disk, and then 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 QuTS hero 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 Manager** > **Disks** > **Device**, select a disk, and then 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.
Securely erase	Go to **Storage Manager** > **Disks** > **Device**, select a free disk, and then click **Action** > **Secure Erase**. Permanently erases all data on a disk. For details, see Securely erasing a disk.
View disk information	Go to **Storage Manager** > **Disks** > **Device**, and then select a disk. Displays disk details such as hardware information, statuses, disk health information such as S.M.A.R.T., and more.

Action	User Action
Configure disk settings	Go to **Storage Manager** > **Disks** > **Device**, select a disk, and then click **Action** > **Disk Settings**. You can configure settings such as a high temperature alarm or Native Command Queuing (NCQ).
Run or schedule S.M.A.R.T. tests	Go to **Storage Manager** > **Disks** > **Disk**, and then perform one of the following: • Select one or more disks, click **Run Test**, and then select **Rapid Test** or **Complete Test**. • Click **Schedule Tests** and go to the **S.M.A.R.T.** tab. For details, see Disk S.M.A.R.T. tests.
Run or schedule performance tests	Go to **Storage Manager** > **Disks** > **Disk**, and then perform one of the following: • Select one or more disks, click **Run Test**, and then select **Sequential Read Test** or **IOPS Read Test**. • Click **Schedule Tests** and go to the **Performance** tab. For details, see Disk performance tests.

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.

Note
To perform this action, you must be logged in as an administrator.

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

1. Go to **Storage Manager** > **Disks** > **Device**.
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. Select an erase mode.

Mode	Description
Fast Erase	QuTS hero 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.
Complete Erase	QuTS hero 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.
SSD Erase	QuTS hero 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.

6. Click **Apply**.
   A confirmation window opens.
7. Enter your password.
8. Click **OK**.

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

Disk S.M.A.R.T. tests

QuTS hero can test the electrical and mechanical properties of your disks, and a small portion of the disk surface or the full disk surface.

Running S.M.A.R.T. tests can help identify any errors or potential issues within a disk. This allows users to take preventive measures before the disk fails and data loss occurs.

Running disk S.M.A.R.T. tests manually

Note
If a S.M.A.R.T. test or performance test is currently running on the disk, you must wait for the test to complete before you can run another test.

1. Go to **Storage Manager** > **Disks** > **Disk**.
2. Select one or more disks.

3. Click **Run Test** and select a S.M.A.R.T. test type.

Test Type	Description
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.

   A confirmation message appears.

4. Click **OK**.

QuTS hero runs the test on the selected disks and then displays the results in the `S.M.A.R.T.` column.

Running disk S.M.A.R.T. tests on a schedule

1. Go to **Storage Manager** > **Disks** > **Disk**.
2. Click **Schedule Tests**.
   The **Schedule Disk Tests** window opens.
3. Go to the **S.M.A.R.T.** tab.
4. Next to **Device**, select the NAS or a connected external enclosure.
5. Next to **Disk**, select a disk.
6. Click a S.M.A.R.T. test type.

Test Type	Description
Rapid S.M.A.R.T. 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 S.M.A.R.T. Test	Tests the electrical and mechanical properties of the disk, and the full disk surface. This test duration varies depending on the storage environment.

7. Depending on the test type, select one of the following:
   - **Enable rapid test**
   - **Enable complete test**
8. Select a frequency.
   - **Daily**: Runs the test once a day.
   - **Weekly**: Runs the test once a week. Select a day of the week.
   - **Monthly**: Runs the test once a month. Select a day of the month.

9. Next to **Time**, specify the time of day to the run the test.
10. Click **Apply**.

QuTS hero runs the selected test on the selected disks according to the configured schedule, and displays the results in the `S.M.A.R.T.` column.

Disk performance tests

QuTS hero 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

Note

If a S.M.A.R.T. test or performance test is currently running on the disk, you must wait for the test to complete before you can run another test.

1. Go to **Storage Manager** > **Disks** > **Disk**.
2. Select one or more disks.
3. Click **Run Test** and select a performance test type.

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

   A confirmation message appears.
4. Click **OK**.

QuTS hero runs the test on the selected disks and then displays the results in the `Sequential Read` or `IOPS Read` column.

Testing disk performance on a schedule

Scheduled performance tests are only available for sequential read, and are run every Monday at 6:30 AM.

1. Go to **Storage Manager** > **Disks** > **Disk**.

2. Select one or more disks.
3. Click **Schedule Tests**.
   The **Schedule Disk Tests** window opens.
4. Go to the **Performance** tab.
5. Set **Weekly Test** to **On**.
6. Click **Apply**.

QuTS hero runs a sequential read test on the selected disks every Monday at 6:30 AM, and displays the results in the `Sequential Read` column.

Disk failure prediction

QuTS hero 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.
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 Manager** >  > **Disk Health**.

   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 Manager** > **Disks** > **Device**, 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.

Status	Description
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.
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.

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 shared folders can be created on a storage pool, enabling you to divide the storage space among different users and applications.
- Disks of different sizes and types can be mixed into one large storage space.
- Disks from connected expansion units can be mixed with disks 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.
- Snapshots can be used with storage pools. Snapshots record the state of the data in a shared folder 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.

Tip

For tiered storage pools, see Qtier hero storage pools.

The system pool

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

Tip
To ensure system performance and stability, the system pool should consist of only SSDs.

Creating a storage pool

Note

- To create a Qtier hero storage pool, see Qtier hero storage pool creation.
- For storage pools created in QuTS hero h5.0.0 or later, if you downgrade the firmware or migrate the pool to a NAS running QuTS hero h4.5.4 or earlier, the system will not be able to import the pool.
- For storage pools containing shared folders where read acceleration has been enabled, the system will not be able to import the pool if you downgrade the firmware or migrate the pool to a NAS running QuTS hero h5.0.0 or earlier.
  For details, see "Enable Read Acceleration" in Shared folder management.

1. Go to **Storage Manager** > **Storage Space**.
2. Click **Create** > **New Storage Pool**.
   The **Create Storage Pool** wizard opens.
3. Select a storage device.
   By default, the current NAS is selected. You can also select an expansion unit connected to the NAS.

   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.
4. Optional: Next to **Pool security**, select **SED secure storage pool**.
   This option is only available when there are SEDs in the selected enclosure.
   The list of disks only displays SEDs.

5. Select a disk type.

   Note
   QuTS hero assigns the first storage pool created as the system pool. The system pool should consist of only SSDs.

6. Select a RAID type.
   Different RAID types require different numbers of disks. You can only select the RAID types for which there are adequate free disks of the selected disk type. QuTS hero 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.

7. Click **Next**.

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
   - 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.

9. Select a usage type for each disk.
   - **Data**: The disk will be used for data storage.
   - **Spare**: The disk will be used as a spare disk. When a data disk in the RAID group fails, the system can automatically replace the failed disk with the spare disk to rebuild the RAID group.

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 a pool description.
13. Configure any of the following settings.

Setting	Description
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 QuTS hero has created the RAID group. **Note** SSD over-provisioning is automatically enabled if QNAP SSD Antiwear Leveling (QSAL) is enabled.
External device SSD over-provisioning	External device SSD over-provisioning reserves the specified percentage of space on each disk in the RAID group to improve write performance and extend the disk's lifespan. **Note** • This setting is available if the selected SSDs are installed in certain QNAP external device models. • This setting can only be configured for RAID types other than JBOD and RAID 0.
Pool over-provisioning	Storage pool over-provisioning reserves the specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool.
Pool guaranteed snapshot space	Reserve a percentage of the total storage pool space for snapshots.

Setting	Description
Alert threshold	QuTS hero issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
Encryption password **Note** This setting is only available when creating an SED secure storage pool.	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.
Auto unlock on startup **Note** This setting is only available when creating an SED secure storage pool.	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.

Setting	Description
QNAP SSD Antiwear Leveling	QNAP SSD Antiwear Leveling (QSAL) is a patented QNAP technology that helps prevent SSDs in the same RAID group from failing at the same time. It works by adding a varying amount of over-provisioning to each SSD, which causes each disk to wear at a different rate. For details, see QNAP SSD Antiwear Leveling (QSAL). **Note** • QSAL is available for the following RAID types: RAID 5, 6, 50, 60, TP. • The RAID group must contain at least two SSDs that can provide estimated life remaining. • At least one SSD must have over 3% estimated life remaining.
Optimize performance	The system will optimize the pool's storage performance immediately after the pool is created. **Important** • This setting optimizes storage performance for disks over 10 TB. We recommend enabling this setting only when using such disks. • Storage pool optimization requires at least 100 GB of free pool space. • Optimizing pool performance takes several minutes. During optimization, the pool is unavailable and you cannot create another pool with this setting also enabled.

14. Click **Next**.
15. Verify the storage pool information.
16. Click **Create**.
    A confirmation message appears.
17. Click **OK**.

QuTS hero creates the storage pool.

Storage pool management

To open the management page of a storage pool, go to **Storage Manager** > **Storage Space**. Identify the pool, and then under **Action**, click ⋮ > **Manage**.

Tabs

Tab	Description
Usage	Displays space usage details.
RAID	Displays RAID group information and actions.
Qtier hero (Qtier hero storage pools only)	Displays tiering information.
Statistics	Displays utilization statistics.
Data Reduction	Displays data reduction statistics.
Installed Apps	Displays information on all apps installed in the pool.
Properties	Displays all pool properties and configured settings.

Pool actions

Click **Action**, and then select an option.

Action	Description
Set Threshold	Allows you to configure alerts when pool space exceeds a specified threshold. For details, see Configuring storage pool space alerts.
Configure Pool Guaranteed Snapshot Space	Allows you to configure a dedicated space in the pool for storing snapshots. For details, see Configuring pool guaranteed snapshot space.
Configure Pool Over-Provisioning	Configures the amount of pool space to reserve for over-provisioning. For details, see Configuring storage pool over-provisioning.
Configure Pool Spare Disks	Allows you to assign free disks as spare disks for the pool.

Action	Description
Resync Priority	Allows you to select a different resync priority that affects RAID operation speeds when the NAS is in use. For details, see Configuring storage pool resync priority.
Set Tiering Schedule (Qtier hero storage pools only)	Allows you to configure a tiering schedule and a minimum retention time for recently accessed data stored in the fastest tier. For details, see Configuring a tiering schedule.
Manage Tiering Settings (Qtier hero storage pools only)	Allows you to view and adjust tiering settings for each shared folder and LUN in the Qtier hero storage pool, including the target tier and write acceleration mode. For details, see Configuring tiering settings for Qtier hero shared folders and LUNs.
Edit Description	Edits the pool description.
Expand Pool	Allows you to expand the pool by adding a new RAID group or adding disks to a RAID group. For details, see Expanding a storage pool by adding a new RAID group and Expanding a storage pool by adding disks to a RAID group. **Note** To expand a pool by replacing disks in a RAID group, see Expanding a storage pool by replacing disks in a RAID group.
Free some space	Allows to perform one or more actions to increase free space in the pool. For details, see Increasing free space in a storage pool.
SED Settings	Allows you to perform encryption-related actions on an SED secure storage pool. For details, see SED storage pool actions.
Safely Detach Pool	Safely detaches the pool from the system.
Pool Scrubbing	Scans the file system of each RAID group in the pool and automatically repairs any bad blocks. For details, see Scrubbing a storage pool.
Clean Dedup Table	Removes unused entries from the deduplication table, which is used for recording duplicate data in the pool.

Action	Description
Remove Pool	Deletes the storage pool. For details, see Deleting a storage pool.

Storage pool status

You can view storage pool statuses in **Storage Manager** > **Storage Space**.

Status	Description
Ready	The storage pool is working normally. All RAID groups in the pool have the status `Online`.
Creating	The system is creating the storage pool.
Cleaning	The system is cleaning the deduplication table.
Error	One or more RAID groups in the storage pool have the status `Failed`. **Note** It might be possible to recover some data from shared folders and LUNs.
Expanding	The system is expanding the capacity of the storage pool.
Importing	The system is attaching and recovering the detached storage pool.
Locked	The SED secure storage pool is locked.
Locking	The system is locking the SED secure storage pool.
Migrating	The system is expanding the capacity of the storage pool, where one or more RAID groups in the pool are undergoing RAID migration (change in RAID type).
Optimizing	The system is optimizing the storage pool's storage performance after pool creation. This status appears if you selected **Optimize performance** in the pool creation wizard.
Read Only	The storage pool allows read operations only.
Rebuilding	One or more RAID groups in the storage pool have the status `Rebuilding`. QuTS hero is currently rebuilding them due to disk failure.

Status	Description
Removing	The system is deleting the storage pool.
Safely Detaching	The system is safely detaching the storage pool from the system.
Scrubbing	The system is scrubbing the storage pool.
Unlocking	The system is unlocking the SED secure storage pool.
Warning (Degraded)	One or more RAID groups in the storage pool have the status `Degraded`. There are not enough spare disks available to QuTS hero to rebuild all of the RAID groups.
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.
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 storage pool space alerts.

Deleting a storage pool

Only administrators can perform this task.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Manage**.
   The storage pool management page appears.
4. Click **Action**, and then select **Remove Pool**.
   The **Remove Pool** window opens.

5. Enter your password.

   Note
   You must be logged in as an administrator.

6. Select **I understand that all shared folders, LUNs, snapshot vaults, and installed apps in this storage pool will be removed**.

   Warning
   All data in the storage pool will be deleted.

7. Click **Remove**.

Scrubbing a storage pool

Scrubbing a storage pool scans the file system of each RAID group in the pool. QuTS hero automatically attempts to repair bad blocks to maintain data consistency.

Important

- While the scrubbing task is running, the read and write performance of the storage pool may be reduced. You should schedule pool scrubbing to run during times of low NAS usage.
- To perform storage pool scrubbing automatically on a schedule, see Storage global settings.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Pool Scrubbing**.
   The **Pool Scrubbing** window opens.
4. Click **OK**.

Configuring storage pool space alerts

Storage pool space alerts allow you to receive timely warnings before free space in a storage pool starts to run out. Besides a low space alert, you can also configure a used space alert with a customized threshold.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Set Threshold**.
   The **Set Threshold** window opens.

4. Configure any of the following settings.

Setting	Description
Alert when used space exceeds alert threshold	When used space in the pool is greater than or equal to the specified threshold, the system sets the pool status to `Warning (Threshold Reached)` and generates a corresponding log entry. **Note** The default threshold value is 80%.
Alert when pool space is low	When pool space runs low, the system sets the pool status to `Warning (Space Low)` and generates a corresponding log entry. **Note** • Insufficient space might affect data storage, snapshot, and application services. • QNAP recommends enabling this setting if there are installed apps, thin shared folders, or thin LUNs in the pool.

5. Click **Apply**.

Configuring storage pool over-provisioning

Storage pool over-provisioning reserves the specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Configure Pool Over-Provisioning**.
   The **Configure Pool Over-Provisioning** window opens.
4. Select **Pool over-provisioning**.
5. Set the percentage of storage pool space to reserve for over-provisioning.

   Tip
   The default value is 10%.

6. Click **Apply**.

Configuring storage pool resync priority

Storage pool resync priority determines the minimum speed of RAID operations in the storage pool.

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.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Resync Priority**.
4. Select one of the following priorities:
   - **Service First (Low speed)**: QuTS hero performs RAID operations at lower speeds in order to maintain NAS storage performance.
   - **Default (Medium speed)**: QuTS hero performs RAID operations at the default speed.
   - **Resync First (High speed)**: QuTS hero performs RAID operations at higher speeds. Users may notice a decrease in NAS storage performance while RAID operations are in progress.

Increasing free space in a storage pool

Storage Manager 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 Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Free some space**.
   The **Increase Pool Free Space** window opens.
4. 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
Delete older snapshots	**a.** Select a shared folder or LUN. **b.** Click **Manage**. The **Snapshot Manager** window opens. **c.** Select one or more snapshots to delete. **d.** Click **Delete**.
Release unused pool guaranteed snapshot space	**Note** Pool guaranteed snapshot space is storage pool space that is reserved for storing snapshots. **a.** Click **Edit**. The **Configure Pool Guaranteed Snapshot Space** window opens. **b.** Select a lower percentage or specify a lower amount of storage pool space to reserve for snapshots. **c.** Click **Apply**.
Release unused shared folder or LUN guaranteed snapshot space	**Note** A shared folder or LUN's guaranteed snapshot space is storage pool space that is reserved for storing snapshots of the shared folder or LUN. **a.** Select a shared folder or LUN. **Note** The amount of unused guaranteed snapshot space you can release is displayed next to the shared folder or LUN name. **b.** Click **Edit**. The **Edit Shared Folder** or **Edit LUN** window opens. **c.** Go to the **General** tab. **d.** Next to **Guaranteed snapshot space**, specify a lower amount of space to reserve for snapshots of the selected shared folder or LUN. **e.** Click **Apply**.

Option	User Action
Release pool over-provisioning space	**Note** Storage pool over-provisioning reserves a specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool. **a.** Click **Edit**. The **Configure Pool Over-Provisioning** window opens. **b.** Specify a lower percentage of storage pool space to reserve for over-provisioning. **c.** Click **Apply**.
Convert a thick shared folder to a thin shared folder	**a.** Select a thick shared folder. **b.** Click **Execute**. The **Convert to Thin Shared Folder** window opens. **c.** Specify a new quota that is lower than the current capacity. **d.** Click **Apply**. The system converts the thick shared folder to a thin shared folder and releases the freed space to the storage pool.
Expand the storage pool	**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.

5. Optional: Perform another available action.
6. Click **Close**.

Storage pool expansion

Expanding a storage pool by adding a new RAID group

You can expand the capacity of a storage pool by creating a new RAID group and adding it to the pool. QuTS hero combines the new group with the other RAID groups in the storage pool using striping (RAID 0).

Important

- The new RAID group must have the same RAID type as all existing RAID groups in the pool.
- Adding a RAID group to a pool may change the RAID type of the pool.
- The storage pool cannot contain any locked shared folder, LUN, or snapshot vault.

The number of required disks for expansion depends on the current RAID type of the specified pool.

Pool RAID Type	Disks Required to Expand Pool	Pool RAID Type After Expansion
RAID 0	≥ 1	RAID 0
RAID 1	2	RAID 10
RAID 5	≥ 3	RAID 50
RAID 6	≥ 4	RAID 60
RAID-TP	≥ 5	RAID-TP
Triple Mirror	Multiple of 3	Triple Mirror
RAID 10	Multiple of 2	RAID 10
RAID 50	≥ 3 for each additional RAID 5 group	RAID 50
RAID 60	≥ 4 for each additional RAID 6 group	RAID 60

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Expand Pool**.
   The **Expand Pool** wizard opens.
4. Select **Create and add a new RAID group**.
5. Click **Next**.
6. Optional: Select an expansion unit from the **Select device** 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. Click **Next**.
9. Review the summary information.
10. Click **Finish**.
    A confirmation message appears.
11. Click **OK**.

QuTS hero begins expanding the storage pool. The status of the pool changes to `Expanding`, and then changes back to `Ready` after expansion 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
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 5, RAID 6, RAID 50, RAID 60, or RAID-TP.
   - 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 storage pool that you want to expand is `Ready` or `Warning (Threshold Reached)`.
   - The storage pool does not contain any locked shared folder, LUN, or snapshot vault.
2. Go to **Storage Manager** > **Storage Space**.
3. Identify a storage pool.
4. Under **Action**, click ⋮ > **Expand Pool**.
   The **Expand Pool** wizard opens.
5. Select **Add new disk(s) to an existing RAID group**.
6. Select a RAID group.
   The group must be of type: RAID 5, RAID 6, RAID 50, RAID 60, or RAID-TP.

7. Click **Next**.
8. 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	60
RAID 60	60
RAID-TP	24

Warning

All data on the selected disks will be deleted.

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

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

Expanding a storage pool by replacing disks in a RAID group

You can increase the maximum storage capacity of a storage pool by expanding a RAID group in the pool. To expand the RAID group you replace one of the group's member disks with a higher-capacity disk, wait for the RAID group to rebuild, then repeat until all of its disks have been replaced. This operation can be performed while the storage pool is online and accessible to users.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.

3. Under **Action**, click ⋮ > **Manage**
   The **Storage Pool Management** window opens.
4. Go to the **RAID** tab.
5. Identify a RAID group.
   The RAID group can be of any type except for RAID 0.
6. Ensure there are no global spare disks assigned to the RAID group's enclosure.

   Tip

   - You can view and disable global enclosure spare disks at **Storage Manager** > **Disks**.
   - Alternatively, you can go to **Storage Manager** > **Storage Space**, identify the storage pool, click ⋮ under **Action**, and then select **Configure Pool Spare Disks** to view and disable hot spare disks.

7. Prepare a number of higher-capacity disks.
   You must prepare one higher-capacity disk for each disk in the RAID group.
8. Replace each disk one at a time.
   a. Remove the disk from the drive bay.
      - The NAS beeps twice.
      - The status of the RAID group changes to `Degraded`.
      - The status of the RAID group's storage pool changes to `Warning(Degraded)`.

   b. Insert a new higher-capacity disk into the same drive bay.
      The NAS beeps twice. Then the status of the disk and RAID group change to `Rebuilding`.
   c. Wait for the RAID group to finish rebuilding.

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

      The RAID group status changes back to `Ready`.
9. Repeat the previous step until all disks in the RAID group have been replaced with higher-capacity disks.

The additional capacity from the new disks is added to the storage pool after the RAID group finishes rebuilding for the final disk.

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 Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮ > **Safely Detach Pool**.
   A confirmation message appears.
4. Click **Yes**.
   The storage pool status changes to `Safely Detaching...`. After the system finishes detaching the pool, the pool disappears from Storage Manager.
5. Remove the drives containing the storage pool from the NAS.
6. Install the drives in the new NAS.
7. On the new NAS, go to **Storage Manager** > **Disks**.
8. Click ⋮ and select **Recover** > **Attach and Recover Storage Pool**.
   The **Attach and Recover Storage Pool** window opens.
9. If you are migrating an SED secure storage pool, unlock the pool.
   a. Select **Unlock with SED password**.
   b. Enter the encryption password.
10. Click **OK**.
    The system scans the disks and detects the storage pool.
11. Click **Apply**.

The storage pool appears in Storage Manager on the new NAS.

QNAP SSD Antiwear Leveling (QSAL)

QNAP SSD Antiwear Leveling (QSAL) is a patented QNAP technology that prevents simultaneous multiple SSD failure in a RAID group in a storage pool. It works by setting a different amount of over-provisioning on each SSD so that they wear at different rates.

To enable QSAL in a storage pool, the pool must contain a RAID group that meets the following requirements:

- The RAID group must be one of the following RAID types: RAID 5, 6, 50, 60, TP.
- The RAID group must contain at least two SSDs that can provide estimated life remaining.
- At least one SSD in the RAID group must have over 3% estimated life remaining.

When QSAL is enabled, the following conditions apply:

- SSD over-provisioning is automatically enabled and set to 5% for the RAID group.
- The performance of the RAID group is reduced to that of an equivalent RAID group with one less disk.

You can enable QSAL for both new and existing storage pools. You can also monitor the life status of SSDs in a QSAL-enabled RAID group.

Action	User Action
Enable QSAL for a new storage pool	For details, see Creating a storage pool.
Enable or disable QSAL for an existing storage pool	1. Go to **Storage Manager** > **Storage Space**. 2. Identify a storage pool containing a QSAL-enabled RAID group. 3. Under **Action**, click ⋮ > **Manage**. The **Storage Pool Management** window opens. 4. Click **QSAL**. **Note** This screen is only available if the storage pool contains a RAID group that meets the requirements. 5. Click the toggle button.

Action	User Action
Monitor SSD life status in a QSAL-enabled RAID group	1. Go to **Storage Manager** > **Storage Space**. 2. Identify a storage pool containing a QSAL-enabled RAID group. 3. Under **Action**, click ⋮ > **Manage**. The **Storage Pool Management** window opens. 4. Click **QSAL**. **Note** This screen is only available if the storage pool contains a RAID group that meets the requirements. 5. Select a RAID group. Storage Manager displays QSAL information on the RAID group. On this screen, you can monitor the estimated remaining life of SSDs, replace an SSD with a spare disk, or configure a spare disk.

Qtier hero storage pools

A Qtier hero storage pool is a tiered storage pool consisting of two or three RAID groups, each group composed of different disk types. Depending on its member disk type, each RAID group forms either a high-speed tier (PCIe/NVMe SSDs), medium-speed tier (SAS/SATA SSDs), or low-speed tier (HDDs). Frequently accessed data is stored in a faster tier, while infrequently accessed data is stored in a slower tier, maximizing the strengths of the different disk types.

With a Qtier hero storage pool, you can configure a retention period before data is moved between tiers. For each shared folder and LUN within the pool, you can also assign a target tier and configure how data reaches the target tier.

Qtier hero benefits

NAS Configuration	Cost	Storage Capacity	Read/Write Performance	Management Effort
All HDDs	Low	High	Low	Low
All SSDs	Very high	Low	High	Low
SSDs and HDDs manually separated into two or more storage pools	Moderate	Medium	High for SSD pool, low for HDD pool	High (an administrator must manually move data between pools)

NAS Configuration	Cost	Storage Capacity	Read/Write Performance	Management Effort
Qtier hero with SSDs and HDDs in one Qtier hero storage pool	Moderate	Medium	High for frequently accessed data	Low (QuTS hero automatically moves data between disks)

Qtier hero requirements

Tier requirements

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

Qtier hero Pool Configuration	Tier Combinations
Two tiers	• High-speed tier + Medium-speed tier • High-speed tier + Low-speed tier • Medium-speed tier + Low-speed tier
Three tiers	High-speed tier + Medium-speed tier + Low-speed tier

Disk requirements

Disk Type	High-Speed Tier	Medium-Speed Tier	Low-Speed Tier
PCIe/NVMe SSD	Supported	-	-
SAS SSD	-	Supported	-
SATA SSD	-	Supported	-
SAS HDD	-	-	Supported
NL-SAS HDD	-	-	Supported
SATA HDD	-	-	Supported

Qtier hero storage pool creation

You can create a new Qtier hero storage pool or convert an existing standard storage pool to a Qtier hero storage pool.

Note

You cannot convert an existing Qtier hero storage pool to a standard storage pool.

Creating a Qtier hero storage pool

Note

- To create a standard storage pool, see Creating a storage pool.
- For storage pools created in QuTS hero h5.0.0 or later, if you downgrade the firmware or migrate the pool to a NAS running QuTS hero h4.5.4 or earlier, the system will not be able to import the pool.
- For storage pools containing shared folders where read acceleration has been enabled, the system will not be able to import the pool if you downgrade the firmware or migrate the pool to a NAS running QuTS hero h5.0.0 or earlier.
  For details, see "Enable Read Acceleration" in Shared folder management.

1. Go to **Storage Manager** > **Storage Space**.
2. Click **Create** > **New Qtier hero Storage Pool**.
   The **Create Qtier hero Storage Pool** wizard opens.
3. Optional: Next to **Pool security**, select **SED secure storage pool**.
   This option is only available when SEDs are installed on the NAS.
4. Configure a tier.
   For tier and disk requirements, see Qtier hero requirements.
   a. Identify a tier.
   b. Click  .
   c. Select 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.

d. Select a RAID type.

> **Note**
>
> - Each tier is an individual RAID group within the Qtier hero storage pool.
> - If a tier is configured with a redundant RAID type (RAID 1 or higher) for one tier, all tiers must also be configured with a redundant RAID type.

> **Tip**
> Use the default RAID type if you are unsure of which option to choose.
> For details, see RAID types.

e. Click **Done**.

5. Configure one to two more tiers.
6. Click **Next**.
7. Configure SED settings
   Skip this step if you are not creating an SED secure storage pool.

Setting	Description
Encryption password	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.

Setting	Description
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.

8. Click **Next**.
9. Configure tiering settings.

Setting	Description
Tiering schedule	Configure a schedule for moving data between tiers. **Note** • To minimize impact on pool performance, select off-peak hours. • If no schedule is configured, data will not be moved between tiers.
Minimum retention time before tiering	Keep recently accessed data in the fastest tier for a specific period to prevent the data from being moved to another tier too soon.

10. Click **Next**.
11. Optional: Specify a pool description.
12. Configure any of the following settings.

Setting	Description
Pool over-provisioning	Storage pool over-provisioning reserves the specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool.
Pool guaranteed snapshot space	Reserve a percentage of the total storage pool space for snapshots.

Setting	Description
Alert threshold	QuTS hero issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.
QNAP SSD Antiwear Leveling	QNAP SSD Antiwear Leveling (QSAL) is a patented QNAP technology that helps prevent SSDs in the same RAID group from failing at the same time. It works by adding a varying amount of over-provisioning to each SSD, which causes each disk to wear at a different rate. For details, see QNAP SSD Antiwear Leveling (QSAL). **Note** • QSAL is available for the following RAID types: RAID 5, 6, 50, 60, TP. • The RAID group must contain at least two SSDs that can provide estimated life remaining. • At least one SSD must have over 3% estimated life remaining.
Optimize performance	The system will optimize the pool's storage performance immediately after the pool is created. **Important** • This setting optimizes storage performance for disks over 10 TB. We recommend enabling this setting only when using such disks. • Storage pool optimization requires at least 100 GB of free pool space. • Optimizing pool performance takes several minutes. During optimization, the pool is unavailable and you cannot create another pool with this setting also enabled.

13. Click **Next**.
14. Verify the storage pool information.
15. Click **Create**.
    A confirmation message appears.
16. Click **OK**.

QuTS hero creates the Qtier hero storage pool.

Converting a standard storage pool to a Qtier hero storage pool

Important
Once a standard storage pool is converted to a Qtier hero storage pool, it cannot be converted back to a standard storage pool.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a storage pool.
3. Under **Action**, click ⋮, and then select **Convert to Qtier hero Storage Pool**.
   The Qtier hero storage pool conversion wizard opens.
   The system automatically assigns existing RAID groups to specific tiers based on the disk types in the RAID group. RAID groups with the following disk types are automatically assigned to the following tiers:
   - HDDs only: Low-speed tier
   - SATA SSDs only: Medium-speed tier
   - NVMe SSDs only: High-speed tier
   - Mix of SATA and NVMe SSDs: Medium-speed tier

   Note
   Tiers that have been automatically assigned by the system cannot be edited.
4. Optional: Configure one or more unassigned tiers.

   Note
   - A Qtier hero storage pool must contain two to three tiers.
   - For tier and disk requirements, see Qtier hero requirements.

   a. Identify an unassigned tier.
   b. Click  .
   c. Select 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.

d. Select a RAID type.

Note

- Each tier is an individual RAID group within the Qtier hero storage pool.
- If a tier is configured with a redundant RAID type (RAID 1 or higher) for one tier, all tiers must also be configured with a redundant RAID type.

Tip
Use the default RAID type if you are unsure of which option to choose. For details, see RAID types.

e. Click **Done**.

5. Click **Next**.
6. Configure tiering settings.

Setting	Description
Tiering schedule	Configure a schedule for moving data between tiers. **Note** • To minimize impact on pool performance, select off-peak hours. • If no schedule is configured, data will not be moved between tiers.
Minimum retention time before tiering	Keep recently accessed data in the fastest tier for a specific period to prevent the data from being moved to another tier too soon.

7. Click **Next**.
8. Verify the storage pool information.
9. Click **Create**.

QuTS hero converts the standard storage pool to a Qtier hero storage pool.

Qtier hero storage pool management

To access the following UI elements, go to **Storage Manager** > **Storage Space**, identify a Qtier hero storage pool, and then under **Action**, click ⋮ > **Manage** to access the pool management page.

Note

For actions and settings applicable to all storage pools, see the following:

- Storage pool management
- Storage pool expansion
- Storage pool migration
- QNAP SSD Antiwear Leveling (QSAL)

UI Element	Description
Qtier hero tab	Displays the current tiering status, tiering schedule, and basic information about each tier.
Action > **Set Tiering Schedule**	Allows you to configure a tiering schedule and a minimum retention time for recently accessed data stored in the fastest tier. For details, see Configuring a tiering schedule.
Action > **Manage Tiering Settings**	Allows you to view and adjust tiering settings for each shared folder and LUN in the Qtier hero storage pool, including the target tier and write acceleration mode. For details, see Configuring tiering settings for Qtier hero shared folders and LUNs.

Configuring a tiering schedule

The tiering schedule determines how frequently and when the system automatically moves data between tiers in a Qtier hero storage pool. You can also configure a minimum retention time for recently accessed data in the fastest tier.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a Qtier hero storage pool.
3. Under **Action**, click ⋮, and then select **Manage**.
   The storage pool management page opens.
4. Click **Action**, and then select **Set Tiering Schedule**.
   The **Set Tiering Schedule** window opens.

5. Optional: Configure a schedule for moving data between tiers.

   > **Note**
   > If no schedule is configured, data will not be moved between tiers.

   a. Select **Tiering schedule**.

   b. Specify the frequency, day, and time.

      > **Tip**
      > To minimize impact on pool performance, select off-peak hours.

6. Optional: Configure a minimum retention time.
   This setting prevents recently accessed data in the fastest tier from being moved to a slower tier too soon, especially if the last access occurs shortly before a scheduled tiering operation. This ensures that frequently used data remains in the highest performance tier with optimal read/write speeds.

   a. Select **Minimum retention time before tiering**.

   b. Next to **Retention time for recently accessed data in the fastest tier**, select a duration.

7. Click **Apply**.

QuTS hero applies the tiering schedule settings.

Configuring tiering settings for Qtier hero shared folders and LUNs

You can manage the tiering settings of all shared folders and LUNs in a Qtier hero storage pool in one location. For each shared folder or LUN, you can specify a target tier and write acceleration mode.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a Qtier hero storage pool.
3. Under **Action**, click ⋮, and then select **Manage**.
   The storage pool management page opens.
4. Click **Action**, and then select **Manage Tiering Settings**.
   The **Manage Tiering Settings** window opens.
5. Configure tiering settings for a shared folder or LUN.

   a. Identify a shared folder or LUN.

   b. Under **Tiering Settings**, select a target tier.
   This setting determines the primary tier in which the shared folder or LUN's data is stored. Select a tier based on how frequently the data is accessed:

Tier	Description
High-speed tier	Uses PCIe/NVMe SSDs for the fastest read/write performance. Ideal for frequently accessed data.
Medium-speed tier	Uses SAS/SATA SSDs for balancing performance and capacity. Suitable for daily operations.
Low-speed tier	Uses SAS/SATA HDDs for long-term storage. Ideal for infrequently accessed data.

c. Under **Tiering Settings**, select a write acceleration mode.

> **Note**
> This setting is unavailable when the high-speed tier is selected as the target tier, in which case the system automatically writes data directly to the high-speed tier and stores the data there.

Write Acceleration Mode	Description
Write-buffer	Data is first written to the fastest tier and then moved to the target tier. This mode is ideal for I/O-intensive applications where you want to fully leverage the speed of SSDs for write operations.
Load-balance	Data is written to the fastest tier and the target tier simultaneously, reducing load on any single tier. This mode is suitable for frequently writing large volumes of data but where read operations are infrequent, such as continuous log archiving.
Direct-write	Data is written directly to the target tier, bypassing the fastest tier (no acceleration). This mode is ideal for situations where both read and write operations are not very frequent, such as creating backups or archiving old data.

6. Optional: Configure tiering settings for other shared folders or LUNs.
7. Click **Apply**.

QuTS hero applies the tiering settings.

Shared folders

A shared folder is a portion of storage space created from the space of a storage pool. Shared folders enable users to store data on the NAS and allow connected clients to access that data.

Tip

- To create and configure shared folders, go to **Storage Manager** > **Storage Space**.
- A QuTS hero shared folder is the same as a QTS volume that contains one shared folder.

Creating a shared folder

Note

For shared folders created in QuTS hero h5.0.1 and later, read acceleration is enabled by default and cannot be disabled.
For details, see "Enable Read Acceleration" in Shared folder management.

1. Go to **Storage Manager** > **Storage Space**.
2. Click **Create**, and then select **New Shared Folder**.
   The **Create Shared Folder** wizard opens.
3. Specify a shared folder name.
   - The name can be in any Unicode language.
   - The maximum length is 64 bytes. In English, this equals 64 characters.
   - The following special characters are not allowed: @ " + = / \ : | * ? < > ; [ ] % , ` ' non-breaking space
   - The last character cannot be a period (.) or space.
   - The name cannot begin with a space or "_sn_".
4. Optional: Specify a description.
   The information is for your reference and is not used by QuTS hero.
5. Select a storage pool.
   The shared folder is created using storage space from this pool.
6. Select a method of space allocation.

Allocation	Description
Thick provisioning	QuTS hero allocates storage pool space when the shared folder is created, ensuring the space is available.

Allocation	Description
Thin provisioning	QuTS hero allocates storage pool space on demand, as data is written to the shared folder. **Note** This option is selected by default.

7. Specify the capacity of the shared folder.
The method of space allocation determines the maximum shared folder capacity.

Method	Maximum Size
Thick provisioning	Less than the amount of free space in the parent storage pool. Some space is reserved for the system.
Thin provisioning	5 PB (5000 TB) **Tip** • Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation. • If you do not specify the folder quota, it will be equal to the storage pool quota.

Note
If the parent storage pool does not contain any existing shared folders, setting the allocated quota to maximum may cause the storage pool size to exceed the pool space alert threshold. If this happens, the pool space alert will be disabled.
To reset the pool space alert, see Configuring storage pool space alerts.

8. Optional: Configure shared folder guaranteed snapshot space.
Shared folder guaranteed snapshot space is storage pool space that is reserved for storing snapshots of a folder. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots for this folder.

Note
This setting is only available for thick shared folders.

9. Click **Advanced Settings**.

10. Optional: Configure shared folder encryption.

Note

- To encrypt data on the shared folder, the system generates a unique encryption key based on the user-defined encryption password. To access data on the shared folder, the shared folder must be unlocked with the encryption password, the encryption key file, or via a KMIP server. You can download the encryption key file later.
- You cannot enable or disable encryption after a shared folder is created.
- Encryption decreases read and write speeds.

a. Next to **Storage Settings**, click  .

b. Next to **Folder Encryption**, click  .

c. Specify an encryption password.
The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed.

Warning
If you forget the encryption password and do not have the encryption key file, the shared folder will become inaccessible and all data in the shared folder will be lost. To download the encryption key file, see Managing shared folder encryption.

d. Verify the password.

e. Optional: Enable **Auto unlock on startup**.

Note

- This setting allows the system to save the encryption key so it can automatically unlock the shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
- By default, the system stores the encryption key on the NAS and unlocks with this key. If you enabled storing encryption keys on a KMIP server, you can choose to store the encryption key on the KMIP server in the next step.
- You can change this setting at any time. For details, see Managing shared folder encryption.

f. Optional: Select an auto unlock option.

> **Note**
> This step is only available when all of the following are true:
>
> - You enabled **Auto unlock on startup**.
> - You enabled KMIP service.
>   For details, see KMIP service.
> - You enabled storing encryption keys on the KMIP server.
>   For details, see Storage global settings.

- **Unlock with encryption key stored on NAS** (default): This option stores the encryption key on the NAS.
- **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server.

11. Optional: Configure WORM (Write Once Read Many).
WORM prevents anyone from modifying or deleting files or folders in the shared folder.

> **Important**
> This setting cannot be modified after shared folder creation.

a. Next to **Security Settings**, click .

b. Next to **WORM**, click .

c. Configure any of the following settings.

Setting	Description
Mode	Select a WORM mode. • **Enterprise** Users can delete the shared folder. • **Compliance** Users cannot delete the shared folder. An administrator must remove the storage pool to delete the WORM shared folder. **Note** You cannot modify the WORM mode after folder creation.

Setting	Description
Lock setting	Configure whether files in the shared folder are to be locked automatically or manually. If you choose to lock files automatically, specify the amount of time to delay locking the file after the file is added to the folder. After this time has passed, the file becomes unmodifiable. If you choose to lock files manually, after a file is added to the folder, you can manually configure the file permissions to read-only at any time. **Note** • You cannot modify the lock setting after folder creation. • The time a file becomes locked might vary from the specified time by +/- 1 minute. • The maximum lock delay time is 168 hours and 59 minutes.
Set retention period	Limit how long WORM applies to each file and folder. Files and folders can be deleted after the specified time period.

12. Optional: Next to **Storage Settings**, click to configure any of the following settings.

Setting	Description
Compression	QuTS hero compresses the data in the shared folder to reduce the size of stored data. Enabling compression also reduces the total number of blocks that QuTS hero needs to read and write, increasing read and write speeds. **Tip** Compression does not impact read/write and processor performance on ZFS file systems. Only disable this setting when necessary.
Deduplication	QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data. **Important** To enable deduplication, your NAS must have at least 16 GB of memory.

Setting	Description
SSD read cache	QuTS hero adds data from this folder to the SSD cache to improve read performance. **Important** Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.
Fast clone	Fast Clone enables QuTS hero to create copies of files faster. It also saves storage space by modifying file metadata, allowing original and copied files to share the same data blocks. **Important** • To enable this setting, **Thin provision** must be selected. • Fast Clone only works when the copied file is created in the shared folder containing the original file. • Fast Clone does not improve the speed of snapshot restoration operations such as restoring files from a snapshot, snapshot revert, and snapshot clone.
ZIL synchronized I/O mode	Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes: • **Auto**: QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • **Always**: All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a small impact on performance. • **None**: 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.

Setting	Description
Performance profile (block size)	Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application. **Tip** The default is 128K.
Target tier	**Note** This setting is only available when the shared folder is in a Qtier hero storage pool. This setting determines the primary tier in which the shared folder's data is stored. Select a tier based on how frequently the data is accessed: • **High-speed tier** Uses PCIe/NVMe SSDs for the fastest read/write performance. Ideal for frequently accessed data. • **Medium-speed tier** Uses SAS/SATA SSDs for balancing performance and capacity. Suitable for daily operations. • **Low-speed tier** Uses SAS/SATA HDDs for long-term storage. Ideal for infrequently accessed data.

Setting	Description
Write acceleration mode	**Note** • This setting is only available when the shared folder is in a Qtier hero storage pool. • This setting is unavailable when the high-speed tier is selected as the target tier, in which case the system automatically writes data directly to the high-speed tier and stores the data there. This setting determines how data reaches the target tier depending on your read/write needs. • **Write-buffer** Data is first written to the fastest tier and then moved to the target tier. This mode is ideal for I/O-intensive applications where you want to fully leverage the speed of SSDs for write operations. • **Load-balance** Data is written to the fastest tier and the target tier simultaneously, reducing load on any single tier. This mode is suitable for frequently writing large volumes of data but where read operations are infrequent, such as continuous log archiving. • **Direct-write** Data is written directly to the target tier, bypassing the fastest tier (no acceleration). This mode is ideal for situations where both read and write operations are not very frequent, such as creating backups or archiving old data.

13. Click **Review and Create**.
14. Review the summary information.
15. Click **Create**.

QuTS hero creates the shared folder.

If you enabled encryption and selected **Unlock with encryption key stored on KMIP server**, the system automatically stores the encryption key on the KMIP server.

You can configure shared folder permissions in Control Panel. For details, see Shared folder permissions.

Shared folder management

To open the management page of a shared folder, go to **Storage Manager** > **Storage Space**. Identify the shared folder, and then under **Action**, click ⋮ > **Manage**.

Tabs

Tab	Description
Usage	Displays space usage details.
Statistics	Displays utilization and data reduction statistics.
Properties	Displays all shared folder properties and configured settings.

Shared folder actions

Click **Action**, and then select an option.

Action	Description
Edit	Opens the shared folder editing window. You can edit the folder name, description, capacity, and storage settings including compression, deduplication, SSD read cache, fast clone, ZIL synchronized I/O mode, performance profile, and alert threshold.
Optimize Read Acceleration	Optimizes the read performance of existing files in the shared folder. **Note** • You must first enable read acceleration. • The amount of time it takes to complete the optimization depends on the number of files in the shared folder.
Enable Read Acceleration	Increases the read speeds of new files. **Note** Once read acceleration is enabled, it cannot be disabled.
Resize Shared Folder	Allows you to resize the shared folder. For details, see: • Expanding a shared folder • Shrinking a shared folder

Action	Description
Convert to Thick	Converts a thin shared folder to a thick shared folder. For details, see Converting to a thick shared folder.
Convert to Thin	Converts a thick shared folder to a thin shared folder. For details, see Converting to a thin shared folder.
Edit Properties	Opens the **Edit Properties** window in Control Panel. For details, see Editing shared folder properties.
Edit Permissions	Opens the **Edit Shared Folder Permission** window in Control Panel. For details, see Editing shared folder permissions.
Encryption	Allows you to perform encryption-related actions on an encrypted shared folder. For details, see Managing shared folder encryption.
Remove	Deletes the shared folder. For details, see Deleting a shared folder.

Managing shared folder encryption

You can perform various actions on an encrypted shared folder, including changing the encryption password, downloading the encryption key file, enabling or disabling **Auto unlock on startup**, and locking or unlocking the folder.

> **Note**
> Encryption can only be enabled during shared folder creation. For details, see Creating a shared folder.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify an encrypted shared folder.
3. Under **Action**, click ⋮ > **Manage**.
   The shared folder management page appears.

4. Perform any of the following actions.

Action	User Action
Change encryption password	**Note** • If the encrypted shared folder contains snapshots, you must remove the snapshots before you can change the password. • The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed. **Important** Changing the encryption password also changes the encryption key. If you previously downloaded an encryption key file, you must download a new encryption key file. If **Store encryption keys on KMIP server** is enabled in the storage global settings, the system will automatically update the encryption key on the KMIP server. **a.** Click **Action** > **Edit**. The **Edit Shared Folder** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Specify a new encryption password and reenter the password. **e.** Click **Apply**.
Download encryption key file	You can use the encryption key file to unlock the encrypted shared folder if you forget the encryption password. **a.** Click **Action** > **Encryption** > **Download Encryption Key**. The **Download Encryption Key** window opens. **b.** Enter the current encryption password. **c.** Click **Apply**.

Action	User Action
Enable **Auto unlock on startup**	Allows the system to automatically unlock the encrypted shared folder when the NAS starts. **a.** Click **Action** > **Edit**. The **Edit Shared Folder** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Select **Auto unlock on startup**. **e.** Select an auto unlock option. • **Unlock with encryption key stored on NAS**: This option stores the encryption key on the NAS. • **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server. This option is only available when KMIP service is configured in Control Panel and **Store encryption keys on KMIP server** is enabled in **Storage Manager** >  > **Storage**. For details, see KMIP service and Storage global settings. **f.** Click **Apply**.
Disable **Auto unlock on startup**	Stops the system from automatically unlocking the encrypted shared folder when the NAS starts. **a.** Click **Action** > **Edit**. The **Edit Shared Folder** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Deselect **Auto unlock on startup**. **e.** Click **Apply**.

Action	User Action

Lock shared folder	**Note**
	• Locking an encrypted shared folder disconnects all existing connections to the shared folder.
	• When an encrypted shared folder is locked, you cannot perform the following actions:
	  • Read and write data to the shared folder
	  • Take snapshots of the shared folder
	a. Click **Action** > **Encryption** > **Lock Shared Folder**.
	A confirmation message appears.
	b. Click **Yes**.

Unlock shared folder	You can unlock an encrypted shared folder with the encryption password, an encryption key file, or via the KMIP server.
	a. Click **Unlock**.
	b. Select a method.
	  • **Input encryption password**: Enter the current encryption password.
	  • **Upload encryption key file**: Click **Browse** to upload the encryption key file.
	  • **Unlock via KMIP server**: This method is only available when the encryption key is stored on the KMIP server and the KMIP server is connected.
	c. Optional: Select **Auto unlock on startup**.
	d. Click **Apply**.

Deleting a shared folder

Note

- If an application such as SnapSync is using the shared folder, you must modify the application to use another folder before deleting the shared folder.
- A shared folder with WORM enabled can only be deleted if the WORM type is **Enterprise**.

1. Go to **Storage Manager** > **Storage Space**.

2. Identify a shared folder.
3. Under **Action**, click ⋮ > **Remove**.
   A confirmation message appears.

   Warning
   All data and snapshots in the shared folder will be deleted.
4. Click **Remove**.

Expanding a shared folder

Expanding a shared folder increases its storage capacity.

Note

- Expansion can be performed while the shared folder is online and accessible to users.
- For a thick shared folder, additional space is allocated from the shared folder's parent storage pool.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a shared folder.
3. Under **Action**, click ⋮ > **Resize Shared Folder**.
   The **Resize Shared Folder** window opens.
4. Specify a new larger capacity for the shared folder.
   Capacity can be specified in megabytes (MB), gigabytes (GB), or terabytes (TB).

Provisioning Type	Maximum Size
Thick provisioning	Less than the amount of free space in the parent storage pool. Some space is reserved for the system. **Tip** Click **Set to Max** to set the new capacity to the maximum calculated by the system.

Provisioning Type	Maximum Size
Thin provisioning	5 PB (5000 TB) **Tip** • Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation. • Click **Set to Pool Capacity** to set the new capacity to the total capacity of the parent storage pool.

5. Click **Apply**.
   The **Shared Folder Resizing Wizard** closes. The shared folder status changes to `Expanding...`.

After expansion is complete, the shared folder's status changes back to `Ready`.

Shrinking a shared folder

Shrinking a shared folder decreases its maximum capacity.

Note

- Users and applications will be unable to access the shared folder until the operation is finished.
- For a thick shared folder, the freed space is returned to the shared folder's parent storage pool.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a shared folder.
3. Under **Action**, click ⋮ > **Resize Shared Folder**.
   The **Resize Shared Folder** window opens.
4. Specify a new smaller capacity for the shared folder.
   Capacity can be specified in megabytes (MB), gigabytes (GB), or terabytes (TB).
5. Click **Apply**.
   The **Shared Folder Resizing Wizard** closes. The shared folder's status changes to `Shrinking...`.

After shrinking is finished, the shared folder's status changes back to `Ready`.

Converting to a thick shared folder

Converting a thin shared folder to a thick shared folder guarantees that the parent storage pool reserves a specified amount of space exclusively for that folder. This prevents other storage usage in the pool from affecting the shared folder's available capacity.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a thin shared folder.
3. Under **Action**, click ⋮ > **Convert to Thin**.
   The **Convert to Thin Shared Folder** window opens.
4. Optional: Specify a new capacity.
5. Click **Apply**.

Converting to a thin shared folder

Converting a thick shared folder to a thin shared folder releases its unused capacity back to the parent storage pool. This can free up pool space for other storage operations. However, the shared folder will no longer have a dedicated space and may be unable to store more data if the pool runs out of free space.

> **Note**
> To retain the dedicated space, consider shrinking the thick shared folder instead. This allows you to release only a portion of its unused capacity. For details, see Shrinking a shared folder.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a thick shared folder.
3. Under **Action**, click ⋮ > **Convert to Thick**.
   The **Convert to Thick Shared Folder** window opens.
4. Optional: Specify a new capacity.
5. Click **Apply**.

Configuring a shared folder space alert

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a shared folder.
3. Under **Action**, click ⋮ > **Edit**.
   The **Edit Shared Folder** window opens.
4. Click **Storage Settings**.
5. Next to **Alert threshold**, click  to enable.

6. Specify an alert threshold.
   QuTS hero issues a warning notification when the percentage of used space is greater than or equal to the specified threshold.
7. Click **Apply**.

Data reduction

QuTS hero supports the following data reduction features:

Feature	Description
Compression	Compression attempts to reduce the size of stored files by removing redundant data within each file. Making files smaller means less storage space is consumed and more files can be stored on the NAS.
Deduplication	Deduplication is a technique for eliminating duplicate copies of repeating data. Deduplication reduces the space required to store files, and can also be applied to network data transfers to reduce the number of bytes sent. **Important** To enable deduplication, your NAS must have at least 16 GB of memory.

Configuring compression and deduplication

Important
Changes to the compression and deduplication settings only affect newly added files. Existing files are not affected.

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a shared folder.
3. Under **Action**, click ⋮ > **Edit**.
   The **Edit Shared Folder** window opens.
4. Go to the **Storage Settings** tab.
5. Optional: Enable or disable compression.
6. Optional: Enable or disable deduplication.
7. Click **Apply**.

Viewing data reduction statistics

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a shared folder.

3. Under **Action**, click ⋮ > **Manage**.
   The shared folder management page appears.
4. Go to the **Statistics** tab.
5. Go to the **Data Reduction** section.

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 QuTS hero 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. QuTS hero 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

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, QuTS hero 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.
- 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	Overview
RAID 0	1 to 16	0	• 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.
RAID 1	2	1	• 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 storing important data.

RAID Type	Number of Disks	Disk Failure Tolerance	Overview
RAID 5	3 to 16	1	• 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. • Ideal for running databases and other transaction-based applications.
RAID 6	4 to 16	2	• 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	• 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	• 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. • Recommended for applications that require high fault tolerance, capacity, and random access performance.

RAID Type	Number of Disks	Disk Failure Tolerance	Overview
RAID 60	8 to 30	2 per disk 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. • Recommended if you need higher fault tolerance than RAID 50.
Triple Mirror	3	2	• An identical copy of data is stored on three disks. • There is no degradation in performance while the RAID group is being rebuilt. • Read performance is increased, but capacity is greatly decreased. • Triple Mirror is suitable for storing critical data.
RAID-TP	5 to 24	3	• Data and parity information are striped across all disks. • The capacity of three disks is lost to store parity information. • RAID-TP adds an extra level of redundancy over RAID 6.

RAID actions

The perform the following actions, go to **Storage Manager** > **Storage Space**, identify a storage pool, click ⋮ > **Manage** under **Action**, go to the **RAID** tab, identify a RAID group, and then click **Manage**.

Action	Description
Recover Storage Pool	Recovers the storage pool and all RAID groups from disk disconnections. For details, see Recovering a RAID group.

Action	Description
Replace Disks One by One	Increases the capacity of the RAID group by replacing all of its disks with higher capacity disks. For details, see Expanding a storage pool by replacing disks in a RAID group. **Note** You can also use this feature to replace working disks for maintenance purposes.

RAID group status

Status	Description
Online	The RAID group is working normally.
Degraded	One or more disks in the RAID group have failed or disconnected. The number of disk failures and disconnections are within the disk failure tolerance of the RAID group. There are not enough spare disks available to QuTS hero to replace all the failed and disconnected disks.
Rebuilding	One or more disks in the RAID group have failed or disconnected. The number of disk failures and disconnections are within the disk failure tolerance of the RAID group. QuTS hero has replaced the failed and disconnected disks with spare disks, and is now rebuilding the RAID group.
Failed	One or more disks in the RAID group have failed or disconnected. The number of disk failures and disconnections 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 QuTS hero performs one of the following actions.

Spare Disk Available	Actions
Yes	• QuTS hero 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 `Online` after rebuilding has finished.

Spare Disk Available	Actions
No	You must replace the failed disk manually. QuTS hero starts rebuilding the RAID group after you have installed a working disk.

Configuring an enclosure spare disk

An enclosure spare disk acts as a hot spare for all RAID groups within a single device (NAS or expansion unit). Under normal conditions, the enclosure spare disk is unused and does not store any data. When a disk in any RAID group within the device fails, the spare disk automatically replaces the faulty disk.

Important
Storage devices (the NAS and expansion units) cannot share enclosure spare disks. A unique spare disk must be assigned to each device.

1. Go to **Storage Manager** > **Disks** > **Disk**.
2. Determine the device to configure an enclosure spare disk.
3. Identify a free disk under the device.
4. Under **Action**, click ⋮ > **Set as Enclosure Spare**.
   A confirmation message appears.
5. Click **OK**.

   Warning
   All data on the selected disk will be deleted.

The disk's usage type displays `Spare`.

Recovering a RAID group

You can recover a RAID group in the event of accidental disk removal or SATA connector failure. When one or more disks are removed or disconnected from a RAID group:

- The status of the parent storage pool changes to `Error`.
- The statuses of all RAID groups in the storage pool change to `Failed`.
- All data on shared folders and LUNs in the storage pool becomes inaccessible.

Important
This recovery action 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 Manager** > **Storage Space**.
3. Identify a storage pool with the status `Error`.
4. Under **Action**, click ⋮, and then select **Manage**.
   The storage pool management page appears.
5. Go to the **RAID** tab.
6. Next to a RAID group, click **Manage**, and then select **Recover Storage Pool**.
   A confirmation window appears.
7. Click **OK**.

QuTS hero starts to recover the RAID group and storage pool.

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 QuTS hero, you can use SEDs to create SED secure storage pools. You can also use SEDs to create regular storage pools, 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 Manager** > **Disks** > **Device** and click an SED.

SED Type	Supported
TCG Opal	Yes

SED Type	Supported
TCG Enterprise	Yes (QuTS hero h5.0.1 and later)
TCG Ruby	Yes (QuTS hero h5.2.0 and later)

Creating an SED secure storage pool

Note

To create a Qtier hero storage pool with SEDs, see Qtier hero storage pool creation.

1. Go to **Storage Manager** > **Storage Space**.
2. Click **Create** > **New Storage Pool**.
   The **Create Storage Pool** wizard opens.
3. Click **Start**.
4. Select a storage device.
   By default, the current NAS is selected. You can also select an expansion unit connected to the NAS.

   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.

5. Next to **Pool security**, select **SED secure storage pool**.
   This option is only available when there are SEDs in the selected enclosure.
   The list of disks only displays SEDs.
6. Select a RAID type.
   QuTS hero 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.

7. Click **Next**.

8. Select one or more SEDs.

   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
   - 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.

9. Select a usage type for each disk.
   - **Data**: The disk will be used for data storage.
   - **Spare**: The disk will be used as a spare disk. When a data disk in the RAID group fails, the system can automatically replace the failed disk with the spare disk to rebuild the RAID group.
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 a pool description.

13. Configure any of the following settings.

Setting	Description
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 QuTS hero has created the RAID group. **Note** SSD over-provisioning is automatically enabled if QNAP SSD Antiwear Leveling (QSAL) is enabled.
External device SSD over-provisioning	External device SSD over-provisioning reserves the specified percentage of space on each disk in the RAID group to improve write performance and extend the disk's lifespan. **Note** • This setting is available if the selected SSDs are installed in certain QNAP external device models. • This setting can only be configured for RAID types other than JBOD and RAID 0.
Pool over-provisioning	Storage pool over-provisioning reserves the specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool.
Pool guaranteed snapshot space	Reserve a percentage of the total storage pool space for snapshots.
Alert Threshold	QuTS hero issues a warning notification when the percentage of used pool space meets or exceeds the specified threshold.

Setting	Description
Encryption password	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.
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.
QNAP SSD Antiwear Leveling	QNAP SSD Antiwear Leveling (QSAL) is a patented QNAP technology that helps prevent SSDs in the same RAID group from failing at the same time. It works by adding a varying amount of over-provisioning to each SSD, which causes each disk to wear at a different rate. For details, see QNAP SSD Antiwear Leveling (QSAL). **Note** • QSAL is available for the following RAID types: RAID 5, 6, 50, 60, TP. • The RAID group must contain at least two SSDs that can provide estimated life remaining. • At least one SSD must have over 3% estimated life remaining.

Setting	Description
Optimize performance	The system will optimize the pool's storage performance immediately after the pool is created. **Important** • Storage pool optimization requires at least 100 GB of free pool space. • Optimizing pool performance takes several minutes. During optimization, the pool is unavailable and you cannot create another pool with this setting also enabled.

14. Click **Next**.
15. Verify the storage pool information.
16. Click **Create**.
    A confirmation message appears.
17. Click **OK**.

QuTS hero creates the SED secure storage pool.

SED storage pool actions

To perform the following actions, go to **Storage Manager** > **Storage Space**, identify an SED pool, click ⋮ > **Manage** under **Action**, and then click **Action** > **SED Settings**.

Action	Description
Enable SED Security	Add an encryption password and enable the ability to lock and unlock the pool. The standard pool becomes an SED pool with encryption enabled.
Disable SED Security	Remove the encryption password and disable the ability to lock and unlock the pool. The SED pool becomes a standard pool without encryption.

Action	Description
Change SED Pool Password	Change the encryption password. **Warning** Remember this password. If you forget the password, the pool 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 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 SED pool. All shared folders, LUNs, snapshots, and data in the pool will become inaccessible until the pool is unlocked.
Unlock	Unlock a locked SED pool. All shared folders, LUNs, snapshots, and data in the pool will become accessible.

Removing a locked SED storage pool

1. Go to **Storage Manager** > **Storage Space**.
2. Identify a locked SED secure storage pool.
3. Under **Action**, click ⋮ > **Remove**.
   A confirmation window appears.
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 and then deletes all data. The storage pool is removed from the system. You must enter the encryption password.

Option	Description
Remove pool without unlocking it	This options removes the storage pool without unlocking the disks. The SED disks cannot be used again until you perform one of the following actions: • Unlock the disks. Go to **Storage Manager** > **Disks**, click ⋮, and then select **Recover** > **Attach and Recover Storage Pool**. • Erase the disks using SED erase.

5. Click **Apply**.

The system removes the locked SED storage pool.

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.

Important
You cannot erase a disk if it is the only disk currently in use on the NAS. You must first create another storage pool with one or more other disks.

1. Go to **Storage Manager** > **Disks** > **Disk**.
2. Identify an SED disk.
3. Under **Action**, click ⋮ > **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 an SED, go to **Storage Manager** > **Disks** > **Disk**.

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 Manager** > **Disks** > **Device**, and select an expansion unit to view full hardware details of the expansion unit, including model, serial number, CPU temperature, and system temperature. You can also perform one of the following actions.

Action	Description
Action > **Locate**	Prompt the expansion unit chassis LEDs to blink, so that you can locate the device in a server room or rack.
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.

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 `Failed`.

If you encounter this situation, reconnect the expansion unit to the NAS and QuTS hero will automatically guide you through the recovery process.

You can also perform recovery manually. Go to **Storage Manager** > **Disks**, and then click ⋮ > **Recover** to perform one of the following actions.

Action	Description
Reinitialize Enclosure IDs	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 shared folders, 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 on a QNAP NAS.	• JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10	QNAP NAS running QuTS hero h4.5.0 or later

Storage Mode	Description	Supported RAID Types	Supported Hosts
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. Go to **Storage Manager** > **External Storage**.
2. Identify a RAID enclosure.
3. Under **Action**, 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.
   QuTS hero 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.
    QuTS hero 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 QuTS hero always has sufficient space to store new snapshots.
14. Click **Next**.
15. Click **Create**.
    A confirmation message appears.
16. Click **OK**.

QuTS hero creates the storage pool. You can view and manage it in **Storage Manager** > **Storage Space**.

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. Go to **Storage Manager** > **External Storage**.
2. Identify a RAID enclosure.
3. Under **Action**, 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.
   QuTS hero 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 Manager** > **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 QuTS hero 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**.

QuTS hero formats the RAID group on the external RAID enclosure as an external disk. You can view and manage it in **Storage Manager** > **External Storage**.

QuTS hero external RAID management

Go to **Storage Manager** > **External Storage**, identify a device, and click ⋮ > **Manage** under **Action** to open the device management page.

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	You can select a different device to manage.
Safely Detach	Disconnect a RAID device from the NAS when the device is in NAS Storage mode. QuTS hero stops and then safely removes all storage pools, shared folders, 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, and LUNs on another QNAP NAS, connect the RAID device to the target NAS, go to **Storage Manager** > **Disks**, click ⋮, and then select **Recover** > **Scan All Free Disks**. **Important** This button only appears when the device is in NAS Storage mode.
Eject Enclosure	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.
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 QuTS hero.
Create RAID Group	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.
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.

UI Element	Description
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.
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** screen.

Migrating an external RAID enclosure in NAS storage mode

Follow these steps to move a RAID enclosure containing a storage pool from a QNAP NAS to a different QNAP NAS (which we will call the target NAS).

1. Go to **Storage Manager** > **Disks** > **Device**.
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 Manager** > **Disks**.
8. Click ⋮ > **Recover** > **Attach and Recover Storage Pool**.
   A confirmation message appears.

9. Click **OK**.
   QuTS hero scans the RAID enclosure for storage pools, and then displays them on the **Recover Wizard** window.
10. Click **Apply**.

QuTS hero makes all storage pools, shared folders, and LUNs on the RAID enclosure available on the target NAS at **Storage Manager** > **Storage Space**.

Manually updating external RAID device firmware in QuTS hero

1. Go to **Storage Manager** > **External Storage**.
2. Identify an external RAID device.
3. Under **Action**, click ⋮ > **Manage**.
   The **External Storage Device Management** window opens.
4. Click **Check for Update**.
   The **Firmware Management** window opens. QuTS hero 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 QuTS hero 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 and then power on the device, or to disconnect and then reconnect the device.
   QuTS hero re-detects the device and displays a notification message.
8. Wait for confirmation that the firmware update has finished.
9. Reattach storage pools on the external device to the system.

   Note

   - Updating the firmware on an external device detaches any existing storage pools on the external device from the system. After the update, you must manually reattach the storage pools.
   - You can skip this step if there are no storage pools on the external device.

   a. Go to **Storage Manager** > **Disks**.
   b. Click ⋮ > **Recover** > **Attach and Recover Storage Pool**.

Configuring a spare disk

1. Go to **Storage Manager** > **External Storage**.
2. Identify an external RAID device.
3. Under **Action**, click ⋮ > **Manage**.
   The **External Storage Device Management** window opens.
4. Click **Manage** > **Configure Spare Disk**.
   The **Configure Spare Disk** window opens.
5. Select one or more free disks.
6. 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 Manager** > **Disks**.

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 3.
Configure external storage partitions	Opens **Storage Manager** > **External Storage**. For more information, see Configuring a RAID enclosure as an external storage device.
Create NAS storage space	Opens **Storage Manager** > **Storage Space**. 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 (just a bunch of disks) 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 (small form-factor) 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

Enclosure Type	Description	Supported Platforms	Example Models
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 or USB4 Type-C ports to connect to a NAS or computer.	• Computer: Windows, Linux, macOS • NAS: QTS, QuTS hero	TL-D800C, TL-R1200C-RP, TL-D810TC4

QuTS hero JBOD management

You can manage JBOD enclosures in QuTS hero from the following locations in the Storage Manager utility.

Location	Description
Disks	View, manage, and configure storage for attached JBOD enclosures. You can create storage pools, shared folders, and RAID groups using disks installed in the JBOD enclosure.
External Storage	View and manage attached non-SAS JBOD enclosures and installed disks.

Updating JBOD enclosure firmware in QuTS hero

1. Open Storage Manager.
   QuTS hero periodically checks for the latest firmware for each connected enclosure on login. If a new firmware update is available, QuTS hero 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 and then power on the device, or to disconnect and then reconnect the device.
   QuTS hero re-detects the device and displays a notification message.
3. Wait for confirmation that the firmware update has finished.
4. Reattach storage pools on the external device to the system.

   Note

   - Updating the firmware on an external device detaches any existing storage pools on the external device from the system. After the update, you must manually reattach the storage pools.
   - You can skip this step if there are no storage pools on the external device.

   a. Go to **Storage Manager** > **Disks**.
   b. Click ⋮ > **Recover** > **Attach and Recover Storage Pool**.

Licensing for third-party expansion units

QNAP requires paid licenses for using certain third-party expansion units with a QNAP device. To use these expansion units with full functionality and software support, you must purchase licenses from the QNAP Software Store or within Storage Manager.

You can manage license assignments by going to **Storage Manager** > **Disks** > ⋮ > **Manage Enclosure Licenses**.

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
512 GB	≧ 16 GB

SSD Cache Size	Required Memory
1 TB	≧ 32 GB
2 TB	≧ 64 GB
4 TB	≧ 128 GB
16 TB	≧ 512 GB
30 TB	≧ 1 TB
120 TB	≧ 4 TB

Creating the SSD cache

Note
ZFS ensure that files are sequentially written to the cache, so SSD over-provisioning is not required.

1. Go to **Storage Manager** > **Cache Acceleration**.
2. Click +.
   The **SSD Cache Introduction** window opens.
3. Click **Start**.
   The **Create SSD Cache** window opens.
4. Select a cache type.

Cache Type	Description
Create SSD cache for read and write	QuTS hero creates a combined read cache and write log, which requires fewer SSDs in total. **Note** This setting requires an even number of SSDs.

Cache Type	Description
Create SSD cache for read or write	QuTS hero creates a read cache or a write log separately, which makes each cache more effective. **Note** This setting requires at least 1 SSD for creating the read cache, and at least 2 SSDs or an even number of SSDs for creating the write log.

Important
You cannot change the cache type after the cache has been created. To change the cache type, you must remove and then recreate the SSD cache.

5. Click **Next**.
6. Next to **Cache Type**, select whether to create a read cache or a write log.

   Note
   This option is only available if you previously selected **Create SSD cache for read or write**.

   - **Read Cache**
   - **ZIL Synchronous I/O Write Log**

7. Select one or more SSDs.

   Warning
   All data on the selected disks will be deleted.

8. Click **Next**.
9. Select which shared folders and LUNs can use the read cache.

   Note
   This option is only available if you are creating a read cache or a combined read cache and write log.

   Tip
   This list can be modified later.

10. Select which storage pools can use the write log.

    Note
    This option is only available if you are creating a write log or a combined read cache and write log.

    Tip
    This list can be modified later.

11. Click **Next**.
12. Select a cache mode.

    Note
    This option is only available if you are creating a read cache or a combined read cache and write log.

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**.

13. Click **Next**.
14. Review the summary information.
15. Click **Create**.
    A confirmation message appears.
16. Select **I understand** and then click **OK**.

Configuring SSD cache disks

For details on compatible SSDs, see www.qnap.com/compatibility.

1. Go to **Storage Manager** > **Cache Acceleration**.
2. Go to the **Read Cache** or **ZIL Synchronous I/O Write Log** tab.

   Note
   This step is only available if you created the read cache and write log separately.

3. Click **Manage**, and then select **Configure Cache Disks**.
   The **Configure Cache Disks** window opens.
4. Select the SSDs to be included in the cache.

   Important
   If the cache type is `ZIL Synchronized I/O Write Log` or `Read Cache and ZIL Synchronized I/O Write Log`, you must select an even number of disks.

   Warning
   All data except for system partition data will be deleted.

5. Click **Apply**.
   A confirmation message appears.

QuTS hero uses the selected drives as an SSD cache. If no SSDs are selected, QuTS hero disables the SSD cache.

Configuring cached storage

1. Go to **Storage Manager** > **Cache Acceleration**.
2. Go to the **Read Cache** or **ZIL Synchronous I/O Write Log** tab.

   Note
   This step is only available if you created the read cache and write log separately.

3. Click **Manage**, and then select **Configure Cached Storage**.
4. Select the shared folder and LUNs that are allowed to use the read cache.

   Note
   This option is only available if the cache type is `Read Cache` or `Read Cache and ZIL Synchronous I/O Write Log`.

Important
Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.

5. Select the storage pools that are allowed to use the write log.

Note
This option is only available if the cache type is `ZIL Synchronous I/O Write Log` or `Read Cache and ZIL Synchronous I/O Write Log`.

6. Click **Apply**.

Removing the SSD cache

Note
Removing an SSD from the SSD cache while write caching is enabled may cause data loss.

1. Go to **Storage Manager** > **Cache Acceleration**.
2. Go to the **Read Cache** or **ZIL Synchronous I/O Write Log** tab.

Note
This step is only available if you created the read cache and write log separately.

3. Click **Manage** and then select **Remove**.
   A confirmation message appears.
4. Click **OK**.

QuTS hero flushes all data in the cache to disk, then deletes the RAID groups. This process may take a long time.

External storage

QuTS hero 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 Manager** > **External Storage**. QuTS hero 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.

Action	Description
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 Manager** > **External Storage**.
2. Identify a disk or partition.
3. Under **Action**, click ⋮, 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 **Auto unlock on startup**.
      This enables the system to automatically unlock and mount the encrypted storage space when the NAS starts up. If this setting is disabled, you must specify the encryption password each time the NAS restarts.

Warning

- Enabling this setting 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 QuTS hero 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 **Remote Disk** screen. If a remote disk is disconnected, the disk will become inaccessible and QuTS hero 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 Manager** > **Remote Disk**.
2. Click **Create Remote Disk**.
   The **Create Remote Disk** wizard opens.
3. Specify the IP address of the remote server.
4. Optional: Specify the iSCSI port of the remote server.
5. Click **Connect**.
   QuTS hero 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

File System	Compatible Operating Systems and Devices
HFS+	macOS

Note
The block size of the remote disks is set to 64 k during formatting.

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. Review the settings, and then click **Create**.

QuTS hero adds the remote disk and shares it at **Control Panel** > **Privilege** > **Shared Folders**. By default only the admin account has access.

Remote disk and iSCSI target actions

You can manage remote disks and their iSCSI target connections in **Storage Manager** > **Remote Disk**.

Remote Disk Actions

To view a remote disk, click ⌄ next to an iSCSI target.

To perform an action on a disk, click ⋮ under **Action**, and select an option.

Action	Description
Edit	Allows you to edit the remote disk name.
Delete	Disconnects the remote disk and deletes its shared folder from the local NAS. Existing data on the disk will not be deleted.
Format	Allows you to modify the file system format and I/O setting. For details, see Adding a remote disk.

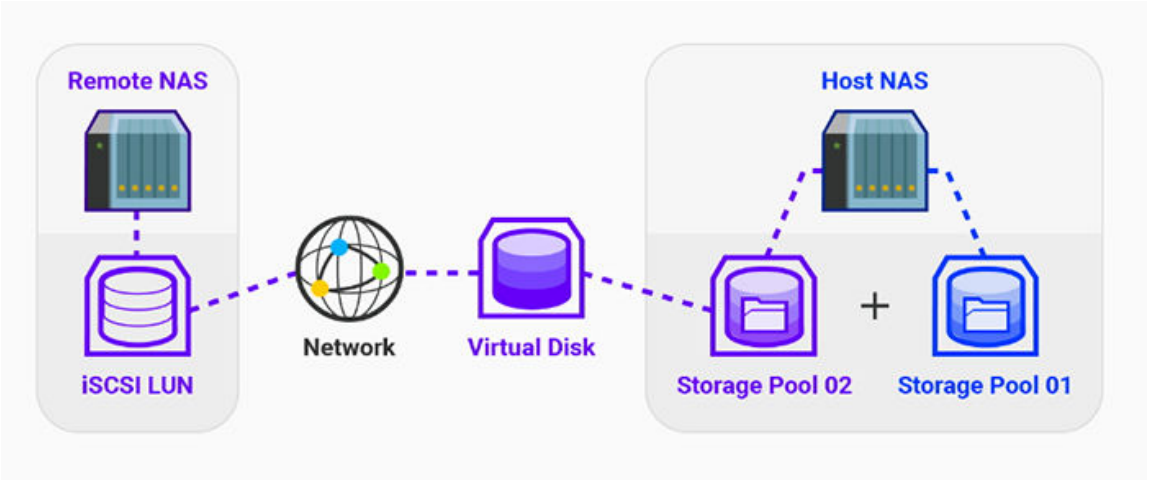
iSCSI Target Actions

To perform an action on an iSCSI target, click ⋮ under **Action**, and select an option.

Action	Description
Edit	Allows you to edit the CHAP authentication and CRC checksum settings for the iSCSI connection. For details, see Adding a remote disk. **Note** You can only edit an iSCSI target when it is disconnected.
Delete	Permanently removes the iSCSI connection, disconnects the remote disk, and deletes its shared folder from the local NAS. Existing data on the disk will not be deleted.
Connect	Connects the iSCSI target.
Disconnect	Disconnects the iSCSI target.

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

- The local and remote NAS devices run the same major version of the same operating system.
- The remote NAS has a storage pool with at least 184 GB of free space, or a free thick LUN with at least 184 GB capacity.

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.

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.
- VJBOD disks only support the RAID type Single.

VJBOD automatic reconnection

If a remote NAS gets disconnected, QuTS hero 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 or IP blocks
  - Incorrect CHAP credentials

VJBOD creation

Creating a VJBOD disk from a new LUN

1. Go to **Storage Manager** > **Disks**.
2. Click ⋮, 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 184 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 selected 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
SSD cache	The SSD cache will be used to improve VJBOD disk access performance.

20. Click **Next**.
    QuTS hero 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 **Create**.
QuTS hero creates the iSCSI target and LUN on the remote NAS, and then creates a VJBOD disk using the LUN. The disk appears in **Storage Manager** > **Disks**.
25. Select a follow-up action.

Action	Description
Create New Storage Pool	Creates a storage pool using the VJBOD disk
Do nothing	Ends the creation process. You can configure the VJBOD disk later. **Tip** To create a storage pool on a VJBOD disk later, go through the normal steps of creating a storage pool. 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 Manager** > **Disks**.
2. Click ⋮, 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.

   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 **Use 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 184 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 **Create**.
    QuTS hero creates a VJBOD disk using the LUN. The disk appears in **Storage Manager** > **Disks**.

21. Select a follow-up action.

Action	Description
Create New Storage Pool	Creates a storage pool using the VJBOD disk
Recover Existing Data	Restores a storage pool that was previously created on the VJBOD disk

Action	Description
Do nothing	Ends the creation process. You can configure the VJBOD disk later. **Tip** To create a storage pool on a VJBOD disk later, go through the normal steps of creating a storage pool. Then on the disk selection screen, under **Enclosure Unit** select `Virtual JBOD`.

22. Click **Finish**.

VJBOD management

VJBOD disk actions

You can manage VJBOD disks by going to **Storage Manager** > **Disks** > **Device**. Select a VJBOD disk, click **Action**, and then select any of the following actions.

Action	Disk Status	Description
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 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 the disconnected VJBOD disk
Re-login	Disconnected	Logs in to the remote NAS again
Edit Target	Disconnected	Edits the following iSCSI target settings: host and remote interfaces, iSER, port number, CHAP authentication, and CRC checksum

Action	Disk Status	Description
Detach	Data	Safely disconnects the VJBOD disk containing a storage pool. You can then connect the LUN to another NAS, create a new VJBOD disk, and recover the pool 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 Manager** > **Disks** > **Device**.
   b. Select the VJBOD disk.
   c. Note the `Remote LUN Name` and `Remote NAS interface`.
2. Detach the VJBOD disk's storage pool.
   a. Go to **Storage Manager** > **Storage Space**.
   b. Identify the storage pool on the VJBOD disk.
   c. Under **Action**, click ⋮, and then select **Manage**.
   The **Storage Pool Management** window opens.
   d. Click **Action**, and then select **Safely Detach Pool**.
3. Remove the VJBOD disk from the NAS.
   a. Go to **Storage Manager** > **Disks** > **Device**.
   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**.
   QuTS hero 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 Manager** > **Disks**.
   b. Click ⋮, 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 **Use 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 **Create**.
QuTS hero creates a VJBOD disk using the LUN. The disk appears in **Storage Manager** > **Disks**.

t. In the actions list, select **Recover Existing Data**.

u. Click **Finish**.

QuTS hero scans for and restores any storage pools, shared folders, 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.

Note

- QuTS hero uses shared folders instead of volumes. For this reason, after creating a VJBOD Cloud volume QuTS hero automatically creates a shared folder with the same name which is stored on the volume. You can then write data to the shared folder.
- In QuTS hero, a VJBOD Cloud volume can only contain one shared folder.

Installing VJBOD Cloud

Requirements:

- A QNAP NAS running QuTS hero h4.5.1 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 QuTS hero as administrator.
2. Ensure that the system pool is configured on the NAS.
For details, see The system pool.
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. Click **OK**.
QuTS hero installs VJBOD Cloud.

VJBOD Cloud volume and LUN creation

Creating a VJBOD Cloud volume

Note

- QuTS hero uses shared folders instead of volumes. For this reason, after creating a VJBOD Cloud volume QuTS hero automatically creates a shared folder with the same name which is stored on the volume. You can then write data to the shared folder.
- A VJBOD Cloud volume can only contain one shared folder.

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**.
   QuTS hero 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	QuTS hero issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.	Specify a value.

Setting	Description	User Actions
Encryption	QuTS hero 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 QuTS hero 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.

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**.

QuTS hero automatically creates a shared folder on the volume. The shared folder has the same name as the volume.

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**.
   QuTS hero 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.

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.

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 QuTS hero 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

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**.
   QuTS hero 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.

Limit	Amount	Notes
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**.

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**.
   QuTS hero 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 QuTS hero 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**.

Cloud Service	Steps
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**.
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**.

Cloud Service	Steps
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.
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**.

Cloud Service	Steps
Google Cloud Storage (OAuth)	1. Select **GoogleCloudStorage**. 2. Select **OAuth**. 3. Specify the project ID. 4. Optional: Select **Validate SSL certificate**.
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**.

Cloud Service	Steps
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**.
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**.

Cloud Service	Steps
Rackspace	1. Select **Rackspace**. 2. Specify the user ID. 3. Specify the password. 4. Optional: Select **Validate SSL certificate**. 5. Select a region.
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	QuTS hero 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	QuTS hero 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	QuTS hero 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 QuTS hero 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** • QuTS hero 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**: QuTS hero 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, QuTS hero 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

QuTS hero 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. Snapshot Manager

> **Note**
> This utility is only accessible to administrators and users with the System Management role.

Snapshot Manager is a QuTS hero utility that helps you create, manage, and monitor snapshots on your NAS. With Snapshot Manager you can perform the following tasks:

- Back up data by taking snapshots
- Recover data from snapshots
- Clone a shared folder or LUN from a snapshot
- Back up snapshots to another location (Snapshot Replica)
- Back up a shared folder or LUN by taking snapshots and syncing the snapshots to a remote NAS (SnapSync)

Snapshots

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

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

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

Snapshot storage limitations

- Maximum snapshots per NAS: 65536
- Maximum snapshots per shared folder or LUN: 65536
- QuTS hero cannot create a new snapshot if there is less than 32 GB of space in the shared folder or LUN's storage pool. To automatically delete old snapshots, enable Smart Snapshot Space Management at Snapshot global settings.

Snapshot global settings

To access the snapshot global settings, go to **Snapshot Manager** >  .

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 shared folder/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 shared folder/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 QuTS hero 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 QuTS hero behavior after a shared folder, 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 vaults, where snapshots of Snapshot Replica jobs are stored at the destination NAS. To set the maximum number of snapshots to retain in a snapshot vault, 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 folders.
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.
Remote Snapshot Replica Connection Timeout	If the remote destination of a Snapshot Replica job does not respond within the timeout period, the system retries. After the specified number of unsuccessful retries, the job fails. We recommend using the default values. • **Timeout (seconds)**: The default value is 600. • **Number of retries**: The default value is 3.

Snapshot creation

Taking a snapshot

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click  .
   The **Take a Snapshot** window opens.

4. Specify a name.
   The name must consist of 1 to 24 characters from the following groups:
   - Letters: A-Z, a-z
   - Numbers: 0-9
   - Special Characters: Dash (-), period (.), underscore (_)
5. Select the snapshot type.
   This setting is only available when taking a snapshot of an NFS shared folder or a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the shared folder or LUN.
Application consistent	The snapshot records the state of all data and applications on the shared folder or LUN. The iSCSI host flushes data in memory to the shared folder or LUN before QuTS hero takes a snapshot. If VMware vCenter is using the shared folder or 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.

6. Optional: Specify a description.
   The description helps you to identify the snapshot.
7. Select a protection policy.

Protection Policy	Description
Allow recycle, Allow delete	The snapshot can be automatically deleted by the system or manually deleted.
Prohibit recycle, Allow delete	The snapshot can never be automatically deleted by the system and can only be manually deleted.
Prohibit recycle and delete until expired	The snapshot can only be automatically deleted by the system or manually deleted after the prohibition expires.

Protection Policy	Description
Prohibit recycle, Prohibit delete until expired	The snapshot can never be automatically deleted by the system and can only be manually deleted after the prohibition expires.

8. Specify the prohibition expiration time.
   This setting is only available when one of the following protection policies is selected:
   - **Prohibit recycle and delete until expired**
   - **Prohibit recycle, Prohibit delete until expired**
9. Click **OK**.

QuTS hero takes the snapshot.

Configuring a snapshot schedule

> **Tip**
> You can configure a separate snapshot schedule for each shared folder and LUN.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Click ⌄.
4. Under **Action**, click ⋮ > **Edit Schedule**.
   The **Edit Snapshot Schedule** window opens.
5. Click  to enable the snapshot schedule.
6. Specify how often the system will take a snapshot.
7. Select the snapshot type.
   This setting is only available when taking a snapshot of an NFS shared folder or a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the shared folder or LUN.

Type	Description
Application consistent	The snapshot records the state of all data and applications on the shared folder or LUN. The iSCSI host flushes data in memory to the shared folder or LUN before QuTS hero takes a snapshot. If VMware vCenter is using the shared folder or 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: Specify a description.
   The description helps you to identify the snapshot.
9. Optional: Enable **Smart snapshots**.
   When enabled, the system only takes a scheduled snapshot if data in the shared folder or LUN has been modified since the last scheduled snapshot was taken. This helps reduce NAS resource usage and the total number of snapshots taken.
10. Select a protection policy.

Protection Policy	Description
Allow recycle, Allow delete	The snapshot can be automatically deleted by the system or manually deleted.
Prohibit recycle, Allow delete	The snapshot can never be automatically deleted by the system and can only be manually deleted.
Prohibit recycle and delete until expired	The snapshot can only be automatically deleted by the system or manually deleted after the prohibition expires.
Prohibit recycle, Prohibit delete until expired	The snapshot can never be automatically deleted by the system and can only be manually deleted after the prohibition expires.

11. Specify the prohibition expiration time.
    This setting is only available when one of the following protection policies is selected:
    - **Prohibit recycle and delete until expired**
    - **Prohibit recycle, Prohibit delete until expired**

12. Optional: Change the snapshot retention policy.

> **Note**
> The snapshot retention policy determines how long QuTS hero keeps each snapshot of a shared folder or LUN before deleting it. Each shared folder and LUN has its own individual snapshot retention policy.

a. Under **Snapshot Retention**, click the retention policy.
The **Local Snapshot Retention Policy** window opens.

b. Select a snapshot retention policy.
Smart Versioning is selected by default.

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, QuTS hero deletes the oldest snapshot when taking a new snapshot.

Snapshot Retention Policy	Description
Smart Versioning	Smart versioning enables you to set the numbers of snapshots to retain for general snapshots and for snapshots of different time periods. For each type of snapshot, once the specified number is reached, each new snapshot replaces the oldest snapshot. Examples: • **General**: 12 - General snapshots are any snapshots taken manually by a user or automatically by the system. When the number of general snapshots reaches 12, the next general snapshot replaces the oldest one. • **Hourly**: 24 - At the start of each hour, the first general snapshot taken within the previous hour becomes an hourly snapshot. When the number of hourly snapshots reaches 24, the next hourly snapshot replaces the oldest one. • **Daily**: 7 - At the start of each day (00:00), the first hourly snapshot of the previous day becomes a daily snapshot. When the number of daily snapshots reaches 7, the next daily snapshot replaces the oldest one. • **Weekly**: 4 - At the start of each week (Monday, 00:00), the first daily snapshot of the previous week becomes a weekly snapshot. When the number of weekly snapshots reaches 4, the next weekly snapshot replaces the oldest one. • **Monthly**: 12 - At the start of each month (day 1, 00:00), the first weekly snapshot of the previous month becomes a monthly snapshot. When the number of monthly snapshots reaches 12, the next monthly snapshot replaces the oldest one.

   c. Click **Apply**.
   The **Local Snapshot Retention Policy** window closes.

13. Optional: Modify the snapshot global settings.

   a. Click **Change settings**.
   The **Global Settings** window appears.

   b. Modify any of the settings.
   For details, see Snapshot global settings.

   c. Click **Apply**.

   d. Click **Close**.

14. Click **Apply**.

QuTS hero starts taking snapshots according to the schedule.

Snapshot management

Editing a snapshot

You can edit the name, description, and protection policy of snapshots taken on the local NAS.

> **Note**
> On the local NAS, you cannot edit snapshots that are stored on a remote NAS or in a snapshot vault, which contains snapshots taken on a remote NAS.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager displays the shared folder or LUN's snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Edit Snapshot**.
   The **Edit Snapshot** window opens.
6. Optional: Edit the snapshot name.
   The name must consist of 1 to 24 characters from the following groups:
   - Letters: A-Z, a-z
   - Numbers: 0-9
   - Special Characters: Dash (-), period (.), underscore (_)
7. Optional: Edit the description.
8. Optional: Select another protection policy.

Protection Policy	Description
Allow recycle, Allow delete	The snapshot can be automatically deleted by the system or manually deleted.
Prohibit recycle, Allow delete	The snapshot can never be automatically deleted by the system and can only be manually deleted.
Prohibit recycle and delete until expired	The snapshot can only be automatically deleted by the system or manually deleted after the prohibition expires. Specify the prohibition expiration time.

Protection Policy	Description
Prohibit recycle, Prohibit delete until expired	The snapshot can never be automatically deleted by the system and can only be manually deleted after the prohibition expires. Specify the prohibition expiration time.

9. Click **Apply**.

QuTS hero saves the changes.

Editing a snapshot schedule

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Click ⌄ to expand the item.
4. Under **Action**, click ⋮ > **Edit Schedule**.
   The **Local Snapshot Schedule** window opens.
5. Click the toggle button to enable or disable the snapshot schedule.
6. Optional: Specify how often the system will take a snapshot.
7. Optional: Select the snapshot type.
   This setting is only available when taking a snapshot of an NFS shared folder or a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the shared folder or LUN.
Application consistent	The snapshot records the state of all data and applications on the shared folder or LUN. The iSCSI host flushes data in memory to the shared folder or LUN before QuTS hero takes a snapshot. If VMware vCenter is using the shared folder or 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: Specify a description.
   The description helps you to identify the snapshot.

9. Optional: Select a protection policy.

Protection Policy	Description
Allow recycle, Allow delete	The snapshot can be automatically deleted by the system or manually deleted.
Prohibit recycle, Allow delete	The snapshot can never be automatically deleted by the system and can only be manually deleted.
Prohibit recycle and delete until expired	The snapshot can only be automatically deleted by the system or manually deleted after the prohibition expires.
Prohibit recycle, Prohibit delete until expired	The snapshot can never be automatically deleted by the system and can only be manually deleted after the prohibition expires.

10. Optional: Specify the prohibition expiration time.
This setting is only available when one of the following protection policies is selected:
    - **Prohibit recycle and delete until expired**
    - **Prohibit recycle, Prohibit delete until expired**

11. Optional: Change the snapshot retention policy.

> **Note**
> The snapshot retention policy determines how long QuTS hero keeps each snapshot of a shared folder or LUN before deleting it. Each shared folder and LUN has its own individual snapshot retention policy.

    a. Under **Snapshot Retention**, click the policy.
    The **Local Snapshot Retention Policy** window opens.

    b. 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, QuTS hero deletes the oldest snapshot when taking a new snapshot.

Snapshot Retention Policy	Description
Smart Versioning	Smart versioning enables you to set the numbers of snapshots to retain for general snapshots and for snapshots of different time periods. For each type of snapshot, once the specified number is reached, each new snapshot replaces the oldest snapshot. Examples: • **General**: 12 - General snapshots are any snapshots taken manually by a user or automatically by the system. When the number of general snapshots reaches 12, the next general snapshot replaces the oldest one. • **Hourly**: 24 - At the start of each hour, the first general snapshot taken within the previous hour becomes an hourly snapshot. When the number of hourly snapshots reaches 24, the next hourly snapshot replaces the oldest one. • **Daily**: 7 - At the start of each day (00:00), the first hourly snapshot of the previous day becomes a daily snapshot. When the number of daily snapshots reaches 7, the next daily snapshot replaces the oldest one. • **Weekly**: 4 - At the start of each week (Monday, 00:00), the first daily snapshot of the previous week becomes a weekly snapshot. When the number of weekly snapshots reaches 4, the next weekly snapshot replaces the oldest one. • **Monthly**: 12 - At the start of each month (day 1, 00:00), the first weekly snapshot of the previous month becomes a monthly snapshot. When the number of monthly snapshots reaches 12, the next monthly snapshot replaces the oldest one.

   c. Click **Apply**.
   The **Local Snapshot Retention Policy** window closes.

12. Optional: Modify the snapshot global settings.

    a. Click **Change settings**.
    The **Global Settings** window appears.

    b. Modify any of the settings.
    For details, see Snapshot global settings.

    c. Click **Apply**.

    d. Click **Close**.

13. Click **Apply**.

QuTS hero starts or stops taking snapshots according to the applied settings.

Viewing snapshot details

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager displays the shared folder or LUN's snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Snapshot Details**.
   The **Snapshot Details** window opens.

Configuring a snapshot retention policy

The snapshot retention policy determines how long QuTS hero keeps each snapshot of a shared folder or LUN before deleting it. Each shared folder and LUN has its own individual snapshot retention policy.

Important
After you create or modify a snapshot retention policy, QuTS hero applies the new policy to existing snapshots. If the new policy is more restrictive than the previous policy, such as changing from keeping for five days to keeping for two days, then QuTS hero deletes existing snapshots to conform with the new policy.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Click .
4. Under **Action**, click > **Edit Retention Policy**.
   The **Local Snapshot Retention Policy** window opens.
5. 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, QuTS hero deletes the oldest snapshot when taking a new snapshot.

Snapshot Retention Policy	Description
Smart Versioning	Smart versioning enables you to set the numbers of snapshots to retain for general snapshots and for snapshots of different time periods. For each type of snapshot, once the specified number is reached, each new snapshot replaces the oldest snapshot. Examples: • **General**: 12 - General snapshots are any snapshots taken manually by a user or automatically by the system. When the number of general snapshots reaches 12, the next general snapshot replaces the oldest one. • **Hourly**: 24 - At the start of each hour, the first general snapshot taken within the previous hour becomes an hourly snapshot. When the number of hourly snapshots reaches 24, the next hourly snapshot replaces the oldest one. • **Daily**: 7 - At the start of each day (00:00), the first hourly snapshot of the previous day becomes a daily snapshot. When the number of daily snapshots reaches 7, the next daily snapshot replaces the oldest one. • **Weekly**: 4 - At the start of each week (Monday, 00:00), the first daily snapshot of the previous week becomes a weekly snapshot. When the number of weekly snapshots reaches 4, the next weekly snapshot replaces the oldest one. • **Monthly**: 12 - At the start of each month (day 1, 00:00), the first weekly snapshot of the previous month becomes a monthly snapshot. When the number of monthly snapshots reaches 12, the next monthly snapshot replaces the oldest one.

6. Click **Apply**.

QuTS hero saves the snapshot retention policy.

Importing a snapshot

You can import a snapshot image file from a local folder or a connected external storage device. You can use the imported snapshot to revert an existing shared folder or LUN, or to create a new shared folder or LUN.

To export a snapshot as a snapshot image file, see Exporting a snapshot.

> **Note**
> You cannot import a snapshot from an ACL 2.0 system to a NAS that uses ACL 1.0.

1. Go to **Snapshot Manager** > **Snapshot**.

2. Click **Import Snapshot**.
   The **Import Snapshot** window opens.
3. Select the source image file.
4. Click **Next**.
5. Select a target.

Option	Description
Revert an existing shared folder or LUN	Reverts an existing shared folder or LUN from the imported snapshot. The system automatically identifies and selects the snapshot's source shared folder or LUN.
Create a new shared folder or LUN	Creates a new shared folder or LUN from the imported snapshot. **a.** Select the destination storage pool. **b.** Specify a name for the new shared folder or LUN.

6. Click **Next**.
7. Review the summary page.
8. Click **Create**.

QuTS hero imports the snapshot.

Exporting a snapshot

You can export a snapshot as a snapshot image file. Later, you can import the snapshot image file on the same NAS or another NAS in order to create a new shared folder or LUN, or revert an existing shared folder or LUN.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager opens the snapshot list of the shared folder or LUN.
4. Identify a snapshot.
5. Under **Action**, click > **Export Snapshot Image File**.
   The **Export Snapshot Image File** window opens.
6. Select a destination.
7. Click **Export**.

QuTS hero exports the snapshot as an image file.

Deleting snapshots

Note

- You cannot delete snapshots with a retention policy that prohibits deletion until the prohibition expires.
- If a snapshot has any associated shared folders or LUNs created via Instant Clone, those shared folders and LUNs must be deleted before you can delete the snapshot.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager displays the shared folder or LUN's snapshot list.
4. Select one or more snapshots.
5. Click **Delete**.
   A confirmation window appears.
6. Click **Apply**.

Snapshot Manager deletes the selected snapshots.

Calculating snapshot size

You can calculate the number of snapshots and their total size in a shared folder 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 **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager displays the shared folder or LUN's snapshot list.
4. Click **Calculate Snapshot Size**.
   The **Calculate Snapshot Size** 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.

Configuring pool guaranteed snapshot space

Pool guaranteed snapshot space is storage pool space that is reserved for storing snapshots. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots.

Pool Guaranteed Snapshot Space Status	Snapshot Storage Location
Disabled	Snapshots are stored in free space in the storage pool.
Enabled	Snapshots are stored in the pool guaranteed snapshot space. If the pool guaranteed snapshot space becomes full, newer snapshots are then stored in free space in the storage pool.

1. Open the configuration page for pool guaranteed snapshot space using one of the following applications.

Application	Actions
Snapshot Manager	**a.** Go to **Snapshot Manager** > **Snapshot**. **b.** Identify a shared folder or LUN. **c.** Under **Action**, click . Snapshot Manager displays the shared folder or LUN's snapshot list. **d.** Click **Pool Guaranteed Snapshot Space**.
Storage Manager	**a.** Go to **Storage Manager** > **Storage Space**. **b.** Identify a storage pool. **c.** Under **Action**, click > **Configure Pool Guaranteed Snapshot Space**.

   The **Configure Pool Guaranteed Snapshot Space** window opens.

2. Select **Enable Pool Guaranteed Snapshot Space**.

3. 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.

4. Click **Apply**.

QuTS hero configures the pool guaranteed snapshot space.

Snapshot data recovery

Restoring files and folders from a snapshot

Tip
Use snapshot revert to quickly restore all data on a shared folder or LUN. For details, see the following topics:

- Reverting a shared folder from a snapshot
- Reverting a LUN from a snapshot

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder or LUN.
3. Under **Action**, click .
   Snapshot Manager displays the snapshot list.
4. Perform one of the following:
   - Select a snapshot, and then click **Open**.
   - Identify a snapshot, click ⋮ under **Action**, and then select **Open**.

   A panel appears, displaying the contents of the snapshot.
5. Select the files and folders to be restored.

6. Perform one of the following actions.

Action	Description
Click **Restore file** > **Restore to Original Location**	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.
Click **Restore file** > **Restore to Selected Location**	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.
Click **Download**	Download the files and folders to your computer in a ZIP file.

QuTS hero restores the files and folders.

Restoring files and folders from a snapshot vault

1. Go to **Snapshot Manager** > **Snapshot Vault**.
2. Identify a snapshot vault.
3. Under **Action**, click .
   Snapshot Manager displays the snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Open**.
   A panel appears, displaying the contents of the snapshot.
6. Select the files and folders to be restored.

7. Perform one of the following actions.

Action	Description
Click **Restore file** > **Restore to Original Location**	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.
Click **Restore file** > **Restore to Selected Location**	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.
Click **Download**	Download the files and folders to your computer in a ZIP file.

QuTS hero restores the files and folders.

Reverting a shared folder from a snapshot

Reverting a shared folder or LUN from a snapshot restores the shared folder or LUN to the state at which the snapshot was taken. Restoring data by reverting the shared folder or LUN from a snapshot is faster than restoring individual files and folders from the snapshot.

You can revert a shared folder from a snapshot stored on either the local NAS or a remote NAS used as the destination for a Snapshot Replica job.

Important

- When reverting a shared folder, the shared folder is inaccessible until the revert process is complete.
- All snapshots taken after the revert point will be deleted.
  If you do not want these snapshots to be deleted, clone the shared folder from the snapshot instead of reverting it from the snapshot. For details, see Cloning a shared folder from a snapshot.
- If the selected snapshot was taken earlier than another snapshot with a protection policy that prohibits deletion, you cannot revert from the selected snapshot until the deletion prohibition on the later snapshot expires.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder.

3. Under **Action**, click .
   Snapshot Manager displays the shared folder's snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Revert Folder Snapshot**.
   The **Revert** window opens.
6. Unlock the shared folder.
   This step only applies if the snapshot source is an encrypted shared folder.
   You must provide the encryption password, encryption key file, or unlock via the KMIP server.
   When the encrypted shared folder is restored, it will be unlocked.
   a. Enter the encryption password, upload the encryption key file, or unlock via the KMIP server.
   b. Optional: Select **Auto unlock on startup**.

      Note
      This setting allows the system to automatically unlock the restored shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
      You can change this setting at any time. For details, see Managing shared folder encryption.
7. Optional: Select **Enable encryption during transfer**.
   This encrypts the snapshot before transferring it for additional security.
8. Click **Revert**.

QuTS hero starts reverting the shared folder from the snapshot. During the process, the status of the shared folder changes to `Reverting`, and QuTS hero disables access to the shared folder until the revert process is finished.

Reverting a LUN from a snapshot

Reverting a shared folder or LUN from a snapshot restores the shared folder or LUN to the state at which the snapshot was taken. Restoring data by reverting the shared folder or LUN from a snapshot is faster than restoring individual files and folders from the snapshot.

You can revert a LUN from a snapshot stored on either the local NAS or a remote NAS used as the destination for a Snapshot Replica job.

Important

- When reverting a LUN, the LUN is inaccessible until the revert process is complete.
- All snapshots taken after the revert point will be deleted.
  If you do not want these snapshots to be deleted, clone the LUN from the snapshot instead of reverting it from the snapshot. For details, see Cloning a LUN from a snapshot.
- If the selected snapshot was taken earlier than another snapshot with a protection policy that prohibits deletion, you cannot revert from the selected snapshot until the deletion prohibition on the later snapshot expires.

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a LUN.
3. Under **Action**, click .
   Snapshot Manager displays the LUN's snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Revert LUN Snapshot**.
   The **Revert** window opens.
6. Unlock the LUN.
   This step only applies if the snapshot source is an encrypted LUN.
   You must provide the encryption password, encryption key file, or unlock via the KMIP server.
   When the encrypted LUN is restored, it will be unlocked.
   a. Enter the encryption password, upload the encryption key file, or unlock via the KMIP server.
   b. Optional: Select **Auto unlock on startup**.

      Note
      This setting allows the system to automatically unlock the restored LUN every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
      You can change this setting at any time. For details, see Managing LUN encryption.
7. Optional: Select **Enable encryption during transfer**.
   This encrypts the snapshot before transferring it for additional security.
8. Click **Revert**.

QuTS hero unmaps the LUN from its iSCSI target and starts reverting the LUN from the snapshot. During the process, the status of the LUN changes to `Reverting`.

Restoring files and folders using Windows Previous Versions

QuTS hero 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, Windows 10, or Windows 11.
- The files must be stored on a shared folder that has at least one snapshot.
- **Enable Windows Previous Versions** must be enabled in the shared folder settings.
- The **Allow symbolic links between different shared folders** option must be enabled by opening SMB Service and going to **SMB Service** > **Advanced** > **Security**.

1. In Windows, open a NAS shared folder using File Explorer.
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 cloning

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

Regular clone and Instant Clone

QuTS hero provides two snapshot clone methods, a regular clone method and Instant Clone. The two clone methods have different advantages and limitations.

Feature	Regular Clone	Instant Clone
Requirements	-	iSCSI service must be enabled in iSCSI & Fibre Channel for cloning LUNs.
Cloning duration	Longer	Shorter
Required space	Normal	Less space required for cloning a thin shared folder or a thin LUN
Cloned shared folders/LUNs can be a source for Snapshot Replica jobs	Yes	No
Cloned shared folders/LUNs can be a source for SnapSync jobs	Yes	No
After cloning, you can revert to an earlier snapshot	Yes	No To revert to an earlier snapshot, you must first delete all shared folders/LUNs that have been cloned from the current snapshot via Instant Clone.
After cloning, the snapshot can be deleted	Yes	No To delete the snapshot, you must first delete all shared folders/LUNs that have been cloned from the snapshot via Instant Clone.
After cloning, the source shared folder/LUN of the snapshot can be deleted	Yes	No To delete the source shared folder/LUN of the snapshot, you must first delete all snapshots that have associated shared folders/LUNs cloned from them via Instant Clone.

Cloning a shared folder from a snapshot

1. Go to **Snapshot Manager** > **Snapshot**.
2. Identify a shared folder.
3. Under **Action**, click .
   Snapshot Manager displays the snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Clone from Snapshot**.
   The **Clone from Snapshot** window opens.

6. Select one of the following:
   - Regular Clone
   - Instant Clone

   For details, see Regular clone and Instant Clone.
   The **Regular Clone** or **Instant Clone** window opens.
7. Specify a shared folder name.
8. Optional: Select a different clone destination.
   This step is only available if you are creating a regular clone.
9. Configure shared folder encryption.
   This steps is only available if the snapshot source is an encrypted shared folder.
   a. Specify an encryption password.
      The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed.

      Warning
      If you forget the encryption password and do not have the encryption key file, the shared folder will become inaccessible and all data in the shared folder will be lost. To download the encryption key file, see Managing shared folder encryption.
   b. Verify the password.
   c. Optional: Enable **Auto unlock on startup**.

      Note
      This setting allows the system to save the encryption key so it can automatically unlock the shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
      You can change this setting at any time. For details, see Managing shared folder encryption.
10. Click **OK**.

QuTS hero clones the shared folder and then displays a confirmation message.

Cloning a shared folder from a snapshot vault

1. Go to **Snapshot Manager** > **Snapshot Vault**.
2. Identify a shared folder snapshot vault.
3. Under **Action**, click  .
   Snapshot Manager displays the snapshot list.
4. Identify a snapshot.

5. Under **Action**, click ⋮ > **Clone from Snapshot**.
   The **Clone from Snapshot** window opens.
6. Select one of the following:
   - Regular Clone
   - Instant Clone

   For details, see Regular clone and Instant Clone.
   The **Regular Clone** or **Instant Clone** window opens.
7. Specify a shared folder name.
8. Optional: Select a different clone destination.
   This step is only available if you are creating a regular clone.
9. Configure shared folder encryption.
   This steps is only available if the snapshot source is an encrypted shared folder.
   a. Specify an encryption password.
      The password must contain 8 to 16 characters, and can be any combination of letters, numbers and special characters. Spaces are not allowed.

      Warning
      If you forget the encryption password and do not have the encryption key file, the shared folder will become inaccessible and all data in the shared folder will be lost.
      To download the encryption key file, see Managing shared folder encryption.
   b. Verify the password.
   c. Optional: Enable **Auto unlock on startup**.

      Note
      This setting allows the system to save the encryption key so it can automatically unlock the shared folder every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
      You can change this setting at any time. For details, see Managing shared folder encryption.
10. Click **OK**.

QuTS hero clones the shared folder and then displays a confirmation message.

Cloning a LUN from a snapshot

1. Go to **Snapshot Manager** > **Snapshot**.

2. Identify a LUN.

   Important
   The LUN must have at least one snapshot.

3. Under **Action**, click  .
   Snapshot Manager displays the snapshot list.

4. Identify a snapshot.

5. Under **Action**, click ⋮ > **Clone from Snapshot**.
   The **Clone from Snapshot** window opens.

6. Select one of the following:

   - Regular Clone
   - Instant Clone

   For details, see Regular clone and Instant Clone.
   The **Regular Clone** or **Instant Clone** window opens.

7. Specify a LUN name.

8. Optional: Select a different clone destination.
   This step is only available if you are creating a regular clone.

9. Configure LUN encryption.
   This steps is only available if the snapshot source is an encrypted LUN.

   a. Specify an encryption password.

      Note
      The password cannot contain the following characters or sequences: space ( ), dollar sign ($), colon (:), equal sign (=), HTML double quote ("), HTML backslash (\)

      Warning
      If the LUN is locked, and you forget the encryption password and do not have the encryption key file, the LUN will become inaccessible and all data in the LUN will be lost.
      To download the encryption key file, see Managing LUN encryption.

   b. Verify the password.

c. Optional: Select **Auto unlock on startup**.

> **Note**
> This setting allows the system to automatically unlock the restored LUN every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
> You can change this setting at any time. For details, see Managing LUN encryption.

10. Click **OK**.

QuTS hero clones the LUN and then displays a confirmation message.

Cloning a LUN from a snapshot vault

1. Go to **Snapshot Manager** > **Snapshot Vault**.
2. Identify a LUN snapshot vault.
3. Under **Action**, click .
   Snapshot Manager displays the snapshot list.
4. Identify a snapshot.
5. Under **Action**, click > **Clone from Snapshot**.
   The **Clone from Snapshot** window opens.
6. Select one of the following:
   - Regular Clone
   - Instant Clone

   For details, see Regular clone and Instant Clone.
   The **Regular Clone** or **Instant Clone** window opens.
7. Specify a LUN name.
8. Optional: Select a different clone destination.
   This step is only available if you are creating a regular clone.
9. Configure LUN encryption.
   This steps is only available if the snapshot source is an encrypted LUN.
   a. Specify an encryption password.

   > **Note**
   > The password cannot contain the following characters or sequences: space ( ), dollar sign ($), colon (:), equal sign (=), HTML double quote ("), HTML backslash (\)

> **Warning**
> If the LUN is locked, and you forget the encryption password and do not have the encryption key file, the LUN will become inaccessible and all data in the LUN will be lost.
> To download the encryption key file, see Managing LUN encryption.

b. Verify the password.

c. Optional: Select **Auto unlock on startup**.

> **Note**
> This setting allows the system to automatically unlock the restored LUN every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
> You can change this setting at any time. For details, see Managing LUN encryption.

10. Click **OK**.

QuTS hero clones the LUN and then displays a confirmation message.

Snapshot Replica

- Snapshot Replica is a snapshot-based full backup solution for QuTS hero.
- With Snapshot Replica you can back up the snapshots of a shared folder or block-based LUN to another storage pool, either on the local NAS or a remote QNAP NAS.
- Backing up data with Snapshot Replica reduces storage space and bandwidth requirements, and simplifies data recovery.
- Backed-up snapshots are stored in snapshot vaults at the destination NAS.

Protection levels

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

- Snapshots only: Take snapshots only.
- Snapshots + Local Snapshot Replica: Take snapshots and back them up to another storage pool on the local NAS.
- Snapshots + Remote Snapshot Replica: Take snapshots and back them up to a remote NAS.

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
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 failure • NAS cannot power on • QuTS hero encounters an error and cannot start	No	No	Yes

Snapshot Replica requirements

Requirements	Source NAS	Destination NAS
Basic requirements	• Must be a QNAP NAS that supports snapshots. • Both source and destination NAS devices must be running QuTS hero. Replicating snapshots from QuTS hero to QTS or vice versa is not supported. • Must have at least 1GB of installed memory. • SSH port 22 and TCP data ports 50100-50199 must be open.	

Requirements	Source NAS	Destination NAS
Additional requirements	-	• The NAS must have at least one storage pool with free space greater than or equal to the size of the shared folder or LUN being backed up. • **Allow SSH connections** must be enabled at **Control Panel** > **Network & File Services** > **Telnet / SSH**. • The ACL version on the destination NAS must be the same or later than the ACL version on the source NAS.

Creating a Snapshot Replica job

Important
When running a Snapshot Replica job for the first time, all data on the shared folder 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 **Snapshot Manager** > **Snapshot Replica**.
2. Click **Create a Replication Job**.
   The **Create a Snapshot Replication Job** wizard opens.
3. Optional: Specify a different job name.
4. Select the source.
   a. Select the source storage pool.
   b. Select the source shared folder or LUN.

      Note
      Shared folders and LUNs created via Instant Clone cannot be used as a source for Snapshot Replica jobs.
5. Select the destination.
   a. Select one of the following.

Destination	User Action
Local	Select **Local** to replicate snapshots to your current NAS.

Destination	User Action
Remote	Select **Remote** to replicate snapshots to a remote NAS. Specify the remote NAS using one of the following methods: • Enter an IP address, hostname, or FQDN. • Click  and then select a NAS from the list of QNAP NAS devices on your local network.

b. Enter the credentials of an administrator account or a user account with the System Management role.

> **Important**
> For security reasons, QNAP does not recommend using the "admin" account.

c. Optional: Specify a port.

> **Tip**
> The default port is 22.

d. Click **Connect**.

> **Important**
> If prompted, complete 2-step verification. This is required if the destination NAS has enabled 2-step verification.

QuTS hero connects to the destination NAS using the specified user account, and checks that there is sufficient storage space.

e. Select the destination storage pool.

6. Click **Next**.

7. Select a backup plan.

Backup Plan	Description
Scheduled	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. **a.** Select a scheduling option: • **Run on repeated schedules**: Configure one or more schedules for the job to run at regular intervals (daily, weekly, monthly). • **Run at specific times**: Configure one or more one-time schedules for the job to run once on the specified date and time for each schedule. **b.** Select a backup method: • **Back up all existing snapshots**: The job replicates all snapshots to the destination. • **Take a new snapshot and back it up**: The job takes a new snapshot and replicates only the new snapshot to the destination.
After taking local snapshots	The replica job runs each time QuTS hero creates the specified number of snapshots (the default value is 1). These snapshots can be created manually or on a schedule. Specify the number of snapshots to take before replicating them to the destination.
Manual	The job only runs when a user starts it.

8. Specify how many replicated snapshots to retain at the destination.
After the specified number is reached, QuTS hero deletes the oldest snapshot each time it replicates a new snapshot.
9. Click **Next**.
10. Optional: Configure transfer settings.

Setting	Description
Encrypt data during transfer	QuTS hero 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.

Setting	Description
Compress data during transfer	QuTS hero 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 rate	QuTS hero limits the job's network bandwidth usage to the specified maximum transfer speed. This helps ensure resources remain available for other tasks and services.
Enable application consistent snapshot support	iSCSI LUN application consistent snapshots are only available for VMware and VSS-aware applications running on a Windows server. For this setting to take effect, you must install QNAP Snapshot Agent on the Windows server.

11. Optional: Export the source data to an external storage device.
    Snapshot Replica jobs transfer data over the network. If your network speed is slow, you can manually export the vault data to an external device, and then import the vault data to the target vault on the remote device.

    a. Select **Manually transfer vault data**.

    b. Select one of the following:

Option	Description
Export data now	Select this option to export the data to an external storage device. 1. Connect an external storage device to the local NAS. 2. Click  . 3. Select the external device.
Do not export (I have an existing copy)	Select this option if you already have a copy of the data on an external storage device.

12. Click **Next**.
13. Review the job information.

14. Optional: Select **Execute backup immediately**.
    When enabled, the job runs immediately after being created or after vault data has been imported to the destination NAS.
15. Click **Create**.

QuTS hero creates the job.

A snapshot vault is created on the destination NAS. To view the snapshot vault, log in to the destination NAS, and go to **Snapshot Manager** > **Snapshot Vault**.

Note

- If you chose to manually transfer vault data, you must import the vault data to the newly created snapshot vault on the destination NAS before the job can start running. For details, see Importing vault data from a remote Snapshot Replica source.
- To manually run the Snapshot Replica job, go to **Snapshot Manager** > **Snapshot Replica**, identify the job, and then click  under **Action**.

Managing a Snapshot Replica job

1. Go to **Snapshot Manager** > **Snapshot Replica**.
2. Identify a Snapshot Replica job.
3. Perform one of the following actions:

Action	User Action
Enable the schedule	Click  .
Disable the schedule	Click  .
Start	Click  .
Stop	Click  .
View snapshot list	Click and select **Snapshot List**.
View job details	Click  .
Edit job settings	Click  .

Action	User Action
Delete	Click ⋮ and select **Delete**.

Snapshot vaults

After creating a Snapshot Replica job, a snapshot vault is created on the destination NAS. Each replica job has its own separate vault for storing snapshots replicated from the job source. You can view and manage snapshot vaults by going to **Snapshot Manager** > **Snapshot Vault**.

For details on Snapshot Replica, see Snapshot Replica.

Managing a snapshot vault

1. Go to **Snapshot Manager** > **Snapshot Vault**.
2. Identify a snapshot vault.
3. Perform one of the following actions:

Action	User Action
Import vault data	Click . For details, see Importing vault data from a remote Snapshot Replica source.
View snapshot list	Click .
View Snapshot Replica job details	Click . **Note** To change the retention period, you must edit the Snapshot Replica job settings on the source NAS. For details, see Managing a Snapshot Replica job.
Remove snapshot vault	Click ⋮ and select **Remove**.

Tip

To restore files and folders, or clone a shared folder or LUN, from a snapshot vault, see the following topics:

- Restoring files and folders from a snapshot vault
- Cloning a shared folder from a snapshot vault
- Cloning a LUN from a snapshot vault

Importing vault data from a remote Snapshot Replica source

If you created a Snapshot Replica job on a remote NAS that replicates snapshots on the remote NAS to your local NAS, and you chose to manually transfer vault data, you must import the data to the newly created snapshot vault on your local NAS before the job can start running.

1. Go to **Snapshot Manager** > **Snapshot Vault**.
2. Identify a new snapshot vault created by a Snapshot Replica job on a remote NAS.
3. Under **Action**, click .
   The **Import Vault Data** window opens.
4. Select the location of the vault data.

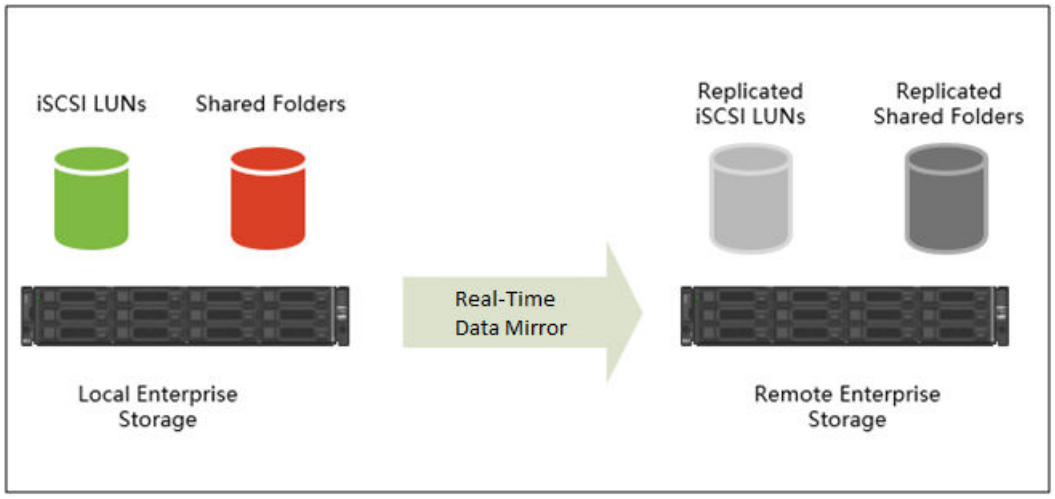
   Note
   If you exported the vault data to an external storage device, ensure the device is connected to the local NAS.

5. Click **Apply**.

Snapshot Manager imports the data to the snapshot vault.

SnapSync

SnapSync is a disaster recovery solution that enables you to back up data from the local NAS to another QNAP NAS using block-level replication in real time. This means that whenever data is written to the source NAS, it is also immediately written to the destination NAS. This reduces the backup time and lowers the risk of data loss.



Note

- To save system resources, you can configure SnapSync to run periodically on a schedule.
- SnapSync encrypts data during transmission using AES-256 encryption.

SnapSync requirements

OS requirements:

SnapSync Job Type	QES Version	QuTS hero Version
QES to QES	QES 2.0.0 or later	N/A
QuTS hero to QuTS hero	N/A	QuTS hero h4.5.2 or later
QES to QuTS hero QuTS hero to QES	QES 2.1.1 Build 20210303 or later	QuTS hero h4.5.2 or later

Other requirements:

- The source and destination shared folders or LUNs must be the same provisioning type (thick or thin).
- If the source and destination NAS devices are running incompatible versions of SnapSync, you will be prompted to update the system firmware on one or both NAS devices to ensure the SnapSync versions are compatible.
  To check the current SnapSync version on a NAS device, go to **Snapshot Manager** > **SnapSync** >  .
- If both the source and destination NAS devices are running QES, they must run the same version of QES to ensure data consistency.
- When using real-time SnapSync, we recommend setting the round-trip latency threshold between the source and destination NAS devices to 5 ms or less. Higher latency might cause local storage write delays.
- For shared folders, the source and destination NAS devices must use the same ACL version (for example, both use ACL 1.0, or both use ACL 2.0).

SnapSync limits and restrictions

SnapSync Limits

The maximum number of SnapSync jobs you can create depends on the backup frequency of the jobs.

SnapSync Job Backup Frequency	Maximum Number of Jobs
Real-time	16
Scheduled and **Manual** (combined)	256

SnapSync Restrictions

The following restrictions apply after creating a SnapSync job.

> **Note**
> Deleting the SnapSync job removes these restrictions.

Action	Source Shared Folder/LUN	Destination Shared Folder/LUN
Edit properties	Allowed	Not Allowed
Edit permissions	Allowed	Allowed
Delete	Not Allowed	Not Allowed
Rename	Not Allowed	Not Allowed
Resize (shrink or expand)	Not Allowed	Not Allowed
Configure guaranteed snapshot space	Not Allowed	Not Allowed
Change provisioning type (thin to thick or thick to thin)	Not Allowed	Not Allowed
Detach parent storage pool	Not Allowed	Not Allowed
Detach parent enclosure	Not Allowed	Not Allowed
Delete parent storage pool	Not Allowed	Not Allowed
Take a snapshot	Allowed User-created snapshots are synced to the destination when the job runs.	Not Allowed

Creating a SnapSync job with a remote NAS as destination

1. Go to **Snapshot Manager** > **SnapSync**.

2. Click **Create a SnapSync Job**.
   The **Create a SnapSync Job** wizard opens.
3. Click **Sync to Remote**.
4. Specify a job name.
   The name cannot contain any of the following special characters: ` * = + [ ] \ | ; : ' " , < > / ? %
5. Select the source storage pool.
6. Select the source shared folder or LUN.

   Note
   Shared folders and LUNs created via Instant Clone cannot be used as a source for SnapSync jobs.

7. Select the destination.
   a. Select one of the following.

Destination	User Action
Local	Select **Local** to replicate snapshots to your current NAS.
Remote	Select **Remote** to replicate snapshots to a remote NAS. Specify the remote NAS using one of the following methods: • Enter an IP address, hostname, or FQDN. • Click  and then select a NAS from the list of QNAP NAS devices on your local network.

   b. Enter the credentials of an administrator account or a user account with the System Management role.

      Important
      For security reasons, QNAP does not recommend using the "admin" account.

   c. Optional: Specify the remote SnapSync port number.

      Tip
      The default is 8080.

   d. Optional: Enable HTTPS encryption.

e. Click **Connect**.

> **Important**
> If prompted, complete 2-step verification. This is required if the destination NAS has enabled 2-step verification.

QuTS hero connects to the destination NAS using the specified user account, and checks that there is sufficient storage space.

8. Click **Next**.
9. Select a backup plan.

> **Note**
> When the source NAS is part of a high-availability cluster, only scheduled and manual SnapSync jobs are supported; real-time SnapSync jobs are not supported.

Backup Plan	Description
Scheduled	SnapSync backs up data periodically, according to the specified schedule.
Real-time	Each write operation to local storage is immediately replicated to the destination storage pool.
Manual	The job only runs when you start it manually.

10. Configure the latency monitor.

> **Note**
> - This setting is only available for real-time SnapSync jobs.
> - Latency Monitor observes the latency of the SnapSync job to ensure the job is running normally. For real-time SnapSync jobs, a higher latency will cause write delays in the local storage. Therefore, we recommend a latency threshold of less than 10 milliseconds (less than 5 milliseconds is optimal).
> - After the SnapSync job is created, you can open Latency Monitor to check the current latency, and then adjust the threshold if necessary. To open Latency Monitor, go to **Snapshot Manager** > **SnapSync**, identify the SnapSync job, and then click ⋮ > **Latency Monitor** under **Action**.

a. Select **Enable latency threshold**.

b. Specify the threshold value, in milliseconds.
The threshold value must be between 0 and 5000 milliseconds.

11. Select the destination storage pool.

12. Select the destination shared folder or LUN.

    Warning
    All data in the shared folder or LUN will be deleted.

    - **Create**: Specify a name for the new shared folder or LUN.
    - **Existing**: Select an existing shared folder or LUN.

13. Optional: Configure job options.

Setting	Description
Encrypt data during transfer	SnapSync encrypts the data during transmission to the destination NAS. The data is then decrypted before being stored at the destination.
Compress data during transfer	SnapSync compresses the data before sending it to the destination. The destination NAS decompresses the data before saving it to disk. Enabling this setting can reduce transfer times if your NAS or the remote NAS has a slow network connection, or the two NAS devices are transferring data via WAN.
Deduplicate data during transfer	SnapSync reduces the amount of storage and bandwidth needed by eliminating duplicate copies of repeated data.
Support application consistent snapshots	SnapSync creates application consistent snapshots. **Note** This option is only available for VMware vCenter and Volume Shadow Copy Service (VSS) aware applications running on a Windows server. For this setting to work, you must install QNAP Snapshot Agent on the Windows server.

14. Click **Next**.

15. Set the source and destination network adapters for this job.
    This step is only available if you selected a remote NAS for the destination.

Adapter Setting	Description
Automatically Select Network Adapter	QuTS hero automatically selects the fastest network adapters at the source and destination for this job. If either network adapter becomes disconnected, QuTS hero will select the fastest available adapter.

Adapter Setting	Description
Manually Select Network Adapter	Manually select the network adapters at the source and destination for this job. You can also select failover adapters, which the job uses if the either primary adapter becomes disconnected. **Note** The source and destination adapter lists only display adapters that can connect to each other.
Specify network IP addresses	Specify the primary and failover IP addresses for the source and destination NAS devices.

16. Click **Next**.
17. Review the job information.
18. Optional: Select **Execute backup immediately**.
    When selected, the job will run immediately after it has been created.
19. Click **Create**.

QuTS hero creates the job.

SnapSync management

You can manage SnapSync by going to **Snapshot Manager** > **SnapSync**.

UI Element	Description
SnapSync Service	Enable or disable the SnapSync service in QuTS hero. You must enable the SnapSync service to create and run SnapSync jobs, and to allow other NAS devices to back up data to this NAS using SnapSync.
Port	Display the port used for incoming and outgoing SnapSync connections.
(**SnapSync Settings**)	Configure SnapSync settings such as the SnapSync port number and upload rate limit. For details, see SnapSync settings.
Create a SnapSync Job	Create a real-time or scheduled SnapSync job. For details, see Creating a SnapSync job with a remote NAS as destination.

UI Element	Description
Performance Test > **Create a SnapSync Performance Test**	Create and run a SnapSync performance test to measure synchronization performance to a remote destination. For details, see Running a SnapSync performance test.
Performance Test > **SnapSync Performance Report**	View the latest SnapSync performance test results. QuTS hero retains the ten most recent SnapSync performance test results.

SnapSync settings

You can access SnapSync settings by going to **Snapshot Manager** > **SnapSync** >  .

In this window, you can view the SnapSync version on the current NAS firmware. If you are having SnapSync compatibility issues, you can check here to ensure that both source and destination NAS devices have the same SnapSync version.

Settings you can configure in this window include the following:

Setting	Action
Port number	Set the port used for incoming and outgoing SnapSync connections. The default port is 874.
Limit upload rate	Limit the amount of upload bandwidth used by SnapSync. Next to **Maximum upload rate (KB/s)**, specify the maximum upload rate in kilobytes per second. If you enter `0`, the upload rate will be unrestricted.

SnapSync job actions

You can perform various SnapSync job actions by going to **Snapshot Manager** > **SnapSync**. Identify a job and select an action under **Operation** or **Action**.

Icon	Action	Description
	Run now	Run the job immediately.
	Stop	Stop a running job.
	Suspend job	Stop a job from running according to its schedule, until a user manually resumes the job.

Icon	Action	Description
	Resume job	Allow a previously suspended job to resume running according to its schedule. If QuTS hero detects that the source and destination folders are different, then it immediately runs the job and synchronizes them.
> **Edit**	Edit	Edit the job's settings. You can edit backup frequency, data transfer, and network adapter settings. **Note** • You cannot change the job's backup frequency from **Scheduled** or **Manual** to **Real-time**, or from **Real-time** to **Scheduled** or **Manual**. • If the account password for the destination NAS changes, then the job will stop working. To resolve this issue, update the password field for the destination NAS account in the job settings. • If the destination IP address changes, then the job state will change to `Disconnected`. To resolve this issue, edit the job setting on the source NAS and then update the destination address.
> **Delete**	Delete	Delete the job.
> **Latency Monitor**	Latency Monitor	Configure the latency threshold. If the job latency goes over the threshold six times within a minute, QuTS hero issues a warning notification. This action is only available for real-time jobs.

Scheduled SnapSync job status

You can check the status of scheduled SnapSync jobs under the `Job Status` column header in **Snapshot Manager** > **SnapSync**.

Tip
Maximize the application window to ensure you can see all columns.

Status	Description
Idle	The job is not currently running.
Starting	SnapSync is preparing to run the job.
Ready	The job is not currently running. This status appears after deleting a SnapSync job, and then creating a new job with the same name and the same source and destination.
Updated	The job has finished running. The source was synchronized to a destination on a remote NAS.
Local Updated	The job has finished running. The source was synchronized to a destination on the local NAS.
Suspended	The job was suspended by a user who clicked **Suspend job** on the source or destination NAS.
Not run yet	The job was created but has not been run.
Updating	The job is running. SnapSync is synchronizing data from the source folder to the destination folder. QuTS hero displays the data transmission speed and synchronization progress as a percentage.
Disconnected	The two NAS devices are disconnected.

Real-time SnapSync job status

You can check the status of real-time SnapSync jobs under the `Job Status` column header in **Snapshot Manager** > **SnapSync**.

Tip
Maximize the application window to ensure you can see all columns.

Status	Description
Ready	The job has been created but has not started synchronizing.
Transferring	The job is running for the first time. SnapSync must transfer all source data to the destination NAS. QuTS hero displays the data transmission speed and synchronization progress as a percentage.

Status	Description
Updating	The job has started running. QuTS hero is synchronizing the source and destination folders.
Updated	The source and destination folders are synchronized.
Aborted	The job has stopped running. The files in the source and destination folders may or may not be identical.
Connection Failed	The two NAS devices are disconnected.
Login Failure	The source NAS is able to connect to the destination NAS, but the username and password saved in the job's settings are invalid.

SnapSync data status

You can view the data status of SnapSync jobs under the `Data Status` column header in **Snapshot Manager** > **SnapSync**.

Tip
Maximize the application window to ensure you can see all columns.

Status	Description
Updating	The job has started running. QuTS hero is synchronizing the source and destination folders. When the job runs for the first time, QuTS hero displays the data transmission speed and synchronization progress as a percentage.
Updated	The source and destination folders are synchronized.
Aborted	The job has stopped running. The files in the source and destination folders are identical. The destination folder is read-only.
Interrupted	The job has stopped running. The files in the source and destination folders are not identical. The destination folder is read-only.
Split	The source and destination folders are no longer paired. The destination folder has full read/write permissions.
[NUMBER] ms	The number indicates the latency of the job in milliseconds. This information is displayed below the data status.

Running a SnapSync performance test

A SnapSync performance test measures synchronization performance to a remote destination. The test results show the performance of SnapSync under current system load.

> **Note**
> To get realistic results, we recommend running the test during regular hours under typical working conditions.

QuTS hero retains the ten most recent SnapSync performance test results. You can review the latest results by going to **Snapshot Manager** > **SnapSync** > **Performance test** > **SnapSync Performance Report**.

1. Go to **Snapshot Manager** > **SnapSync**.
2. Click **Performance test**, and then select **Create a SnapSync Performance Test**.
   The **Create a SnapSync Performance Test** window opens.
3. Specify the destination IP address.

   > **Tip**
   > Click  to view the IP addresses of all QNAP NAS devices on the local network.

4. Specify the system port.

   > **Note**
   > The default port is 8080.

5. Optional: Select **Enable secure connections (HTTPS)**.
6. Specify the username and password of an administrator account on the destination NAS.
7. Click **Connect**.
8. Select the source storage pool.
9. Select the destination storage pool.
10. Select the IP address of the source network adapter.
11. Select the IP address of the destination network adapter.
12. Click **Run Test**.
    A confirmation message window appears.
13. Click **Yes**.
    QuTS hero runs the SnapSync performance test and displays the test results on the **Summary** screen.
14. Click **Finish**.
    The **Create a SnapSync Performance Test** window closes.

To review the results, go to **Snapshot Manager** > **SnapSync** > **Performance test** > **SnapSync Performance Report**.

QNAP Snapshot Agent

QNAP Snapshot Agent is a utility that enables QuTS hero to take application-consistent snapshots of iSCSI LUNs on Microsoft servers, and iSCSI LUNs and NFS shared folders on VMware. Application-consistent snapshots record the state of running applications, virtual machines, and data. When QuTS hero takes a snapshot, QNAP Snapshot Agent triggers the following actions:

- Windows: The server flushes data in memory, logs, and pending I/O transactions to the shared folder or 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**.

To view the list of iSCSI initiators that are using QNAP Snapshot Agent with this NAS, go to **Snapshot Manager** > **Snapshot**. On the **Snapshot** page, click ⋮, and then select **Snapshot Agent**.

Tip

You can unregister a Snapshot Agent connection by clicking 🗑 under **Action**.

9. iSCSI & Fibre Channel

> **Note**
> This utility is only accessible to administrators and users with the System Management role.

iSCSI & Fibre Channel is a QuTS hero 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 iSCSI & Fibre Channel global settings in **Protocol 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**: Specify the IP address or domain name 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.
	• **Enable default iSCSI CHAP**: One-way CHAP forces iSCSI initiators to authenticate when connecting to a target.
	• **Mutual CHAP**: 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.

Setting	Description

Fibre Channel Service	**Enable NPIV service**: NPIV (N_Port ID Virtualization) enables multiple virtual WWPNs on a single Fibre Chanel port for better resource allocation and multi-tenant isolation.
	NPIV service also allows users to use Fibre Channel service in a high-availability (HA) cluster. For details, see NPIV service for high-availability clusters.
	Note
	• This setting is automatically enabled and cannot be disabled when your device is part an HA cluster.
	• When your device is functioning as a standalone device:
	  • Enabling this setting disconnects all existing Fibre Channel connections and removes all Fibre Channel port bindings.
	  • Disabling this setting disconnects all existing Fibre Channel connections.

LUNs

QNAP NAS devices allow other devices to access their storage space in the form of LUNs (logical unit numbers) 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.

Creating a block-based LUN

1. Go to **iSCSI & Fibre Channel** > **LUNs**.
2. Click **Create LUN**.
   The **Create LUN** window opens.
3. Specify a LUN name.
   - Length: 1 to 32 characters
   - Valid characters: 0-9, a-z, A-Z, underscore (_)
4. Optional: Specify a description.
5. Select the storage pool that this LUN will be created in.

6. Select a provisioning type.

Provisioning Type	Description
Thick provisioning	QuTS hero allocates storage pool space when creating the LUN. This space is guaranteed to be available later.
Thin provisioning	QuTS hero 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.

7. Specify a LUN capacity.
The maximum capacity of the LUN depends on the provisioning type:

   - Thick provisioning: Less than the amount of free space in the parent storage pool. Some space is reserved for the system and LUN metadata.
   - Thin provisioning: 5 PB (5000 TB)

   Note

   - For thick LUNs, due to space reserved for system and LUN metadata, the maximum capacity of the LUN is less than the total free space in the storage pool.
   - The maximum capacity displayed is an estimate because the performance profile (block size) setting can affect the final LUN capacity. If you set the LUN capacity to maximum, the final capacity may differ slightly from this figure.

8. Optional: Configure LUN guaranteed snapshot space.
This setting is only available when **Thick** is selected for the provisioning type.

   Note
   LUN guaranteed snapshot space is storage pool space that is reserved for storing snapshots of a LUN. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots for this LUN.

9. Click **Next**.

10. Optional: Configure LUN encryption.

    Note

    - To encrypt data on the LUN, the system generates a unique encryption key based on the user-defined encryption password. To access data on the LUN, the LUN must be unlocked with the encryption password, the encryption key file, or via a KMIP server. You can download the encryption key file later.
    - You cannot enable or disable encryption after a LUN is created.
    - Encryption decreases read and write speeds.

a. Next to **Security Settings**, click .

b. Enable **LUN encryption**.

c. Specify an encryption password.

> **Note**
> The password cannot contain the following characters or sequences: space ( ), dollar sign ($), colon (:), equal sign (=), HTML double quote ("), HTML backslash (\)

> **Warning**
> If the LUN is locked, and you forget the encryption password and do not have the encryption key file, the LUN will become inaccessible and all data in the LUN will be lost.
> To download the encryption key file, see Managing LUN encryption.

d. Verify the password.

e. Optional: Select **Auto unlock on startup**.

> **Note**
> This setting allows the system to save the encryption key so it can automatically unlock the LUN every time the NAS starts, without requiring the user to provide the encryption password or encryption key file.
> You can change this setting at any time. For details, see Managing LUN encryption.

f. Optional: Enable **Auto unlock option**.
Skip this step if you did not select **Auto unlock on startup**.

- **Unlock with encryption key stored on NAS**: This option stores the encryption key on the NAS.
- **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server.
  This option is only available when KMIP service is configured in Control Panel and **Store encryption keys on KMIP server** is enabled in **Storage Manager** > > **Storage**. For details, see KMIP service and Storage global settings.

11. Optional: Next to **Storage Settings**, click to configure any of the following settings.

Setting	Description
Compression	QuTS hero compresses the data in the LUN to reduce the size of stored data. Enabling compression also reduces the total number of blocks that QuTS hero needs to read and write, increasing read and write speeds. **Tip** New shared folders and LUNs have compression enabled by default. Compression does not impact read/write and processor performance on ZFS file systems. Only disable this setting when necessary.
Deduplication	QuTS hero eliminates duplicate copies of data to reduce the required amount of storage space. **Important** To enable deduplication, your NAS must have at least 16 GB of memory.
SSD read cache	QuTS hero adds data from the LUN to the SSD cache to improve read performance. **Important** • This setting is only available when the SSD cache is enabled. • Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.
Fast clone	Fast Clone enables QuTS hero to create copies of files faster. It also saves storage space by modifying file metadata, allowing original and copied files to share the same data blocks. **Important** • Fast Clone only works when the copied file is created in the LUN containing the original file. • Fast Clone does not improve the speed of snapshot restoration operations such as restoring files from a snapshot, snapshot revert, and snapshot clone.

Setting	Description
ZIL synchronized I/O mode	Select the ZFS Intent Log (ZIL) sync setting to improve either data consistency or performance. There are three options: • **Auto (Default)**: QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • **Always**: All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a slight impact on performance. • **None**: 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.
Performance profile (block size)	Specify the block size of the LUN. **Note** The block size affects the maximum LUN size. Smaller block sizes require greater amounts of space to be reserved for LUN metadata.
Target tier	**Note** This setting is only available when the LUN is in a Qtier hero storage pool. This setting determines the primary tier in which the LUN's data is stored. Select a tier based on how frequently the data is accessed: • **High-speed tier** Uses PCIe/NVMe SSDs for the fastest read/write performance. Ideal for frequently accessed data. • **Medium-speed tier** Uses SAS/SATA SSDs for balancing performance and capacity. Suitable for daily operations. • **Low-speed tier** Uses SAS/SATA HDDs for long-term storage. Ideal for infrequently accessed data.

Setting	Description
Write acceleration mode	**Note** • This setting is only available when the LUN is in a Qtier hero storage pool. • This setting is unavailable when the high-speed tier is selected as the target tier, in which case the system automatically writes data directly to the high-speed tier and stores the data there. This setting determines how data reaches the target tier depending on your read/write needs. • **Write-buffer** Data is first written to the fastest tier and then moved to the target tier. This mode is ideal for I/O-intensive applications where you want to fully leverage the speed of SSDs for write operations. • **Load-balance** Data is written to the fastest tier and the target tier simultaneously, reducing load on any single tier. This mode is suitable for frequently writing large volumes of data but where read operations are infrequent, such as continuous log archiving. • **Direct-write** Data is written directly to the target tier, bypassing the fastest tier (no acceleration). This mode is ideal for situations where both read and write operations are not very frequent, such as creating backups or archiving old data.

12. Click **Create**.
    QuTS hero creates the LUN.
    If you enabled encryption and selected **Unlock with encryption key stored on KMIP server**, the system automatically stores the encryption key on the KMIP server.
13. Optional: Map the LUN to a target.
    a. Select **Map to new target**, and then select one of the following:
       - **iSCSI Target**
       - **FC Port Groups**
    b. Select a target.
    c. Optional: Enable the LUN.
       If the toggle switch is enabled, QuTS hero enables the LUN after mapping it to the target.

14. Click **Apply**.
15. Review the summary information.
16. Click **Close**.

Managing LUN encryption

Encryption can only be enabled during LUN creation. For details, see Creating a block-based LUN.

For other actions not related to encryption, see LUN actions.

1. Go to **iSCSI & Fibre Channel** > **LUNs**.
2. Identify an encrypted LUN.
3. Under **Action**, click  > **Encryption**.
   A drop-down menu appears.

4. Perform any of the following actions.

Action	User Action
Change encryption password	**Note** • If the encrypted LUN contains snapshots, you must remove the snapshots before you can change the password. • The password cannot contain the following characters or sequences: space ( ), dollar sign ($), colon (:), equal sign (=), HTML double quote ("), HTML backslash (\) **Important** Changing the encryption password also changes the encryption key. If you previously downloaded an encryption key file, you must download a new encryption key file. If **Store encryption keys on KMIP server** is enabled in **Storage Manager** > > **Storage**, the system will automatically update the encryption key on the KMIP server. **a.** Under **Action**, click > **Edit LUN**. The **Edit LUN** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Specify a new encryption password and reenter the password. **e.** Click **Apply**.
Download encryption key file	You can use the encryption key file to unlock the encrypted LUN if you forget the encryption password. **Note** The encryption key file can only be downloaded when the LUN is unlocked. **a.** Under **Action**, click > **Encryption** > **Download Encryption Key**. The **Download Encryption Key** window opens. **b.** Enter the current encryption password. **c.** Click **Apply**.

Action	User Action
Enable **Auto unlock on startup**	Allows the system to automatically unlock the encrypted LUN when the NAS starts. **a.** Under **Action**, click ⚙ > **Edit LUN**. The **Edit LUN** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Select **Auto unlock on startup**. **e.** Select an auto unlock option. • **Unlock with encryption key stored on NAS**: This option stores the encryption key on the NAS. • **Unlock with encryption key stored on KMIP server**: This option stores the encryption key on the KMIP server. This option is only available when KMIP service is configured in Control Panel and **Store encryption keys on KMIP server** is enabled in **Storage Manager** > ⚙ > **Storage**. For details, see KMIP service and Storage global settings. **f.** Click **Apply**.
Disable **Auto unlock on startup**	Stops the system from automatically unlocking the encrypted shared folder when the NAS starts. **a.** Under **Action**, click ⚙ > **Edit LUN**. The **Edit LUN** window opens. **b.** Go to the **Encryption** tab. **c.** Enter the current encryption password. **d.** Deselect **Auto unlock on startup**. **e.** Click **Apply**.

Action	User Action

Lock LUN	**Note**
	• Locking an encrypted LUN disconnects all existing connections to the LUN.
	• When an encrypted LUN is locked, you cannot perform the following actions:
	  • Read and write data to the LUN
	  • Map the LUN to an iSCSI target
	  • Take snapshots of the LUN
	a. Under **Action**, click ⚙ > **Encryption** > **Lock**.
	A confirmation message appears.
	b. Click **Continue**.

Unlock LUN	You can unlock an encrypted shared folder with the encryption password, an encryption key file, or via the KMIP server.
	a. Under **Action**, click ⚙ > **Encryption** > **Unlock**.
	b. Select a method:
	  • **Input encryption password**: Enter the current encryption password.
	  • **Upload encryption key file**: Click **Browse** to upload the encryption key file.
	  • **Unlock via KMIP server**: This method is only available when the encryption key is stored on the KMIP server and the KMIP server is connected.
	c. Optional: Select **Auto unlock on startup**.
	d. Click **Apply**.

LUN actions

You can perform various actions on LUNs by going to **iSCSI & Fibre Channel** > **LUNs**. Identify a LUN, and then under **Action**, click ⚙ to select the desired action.

For actions related to encryption, see Managing LUN encryption.

To import or export LUNs, see LUN import and export.

LUN Action	Description
Enable LUN	Enable the LUN if it is currently disabled.
Disable LUN	Disable the LUN. The LUN will become inaccessible to connected initiators.
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 an iSCSI target • Mapping a LUN to a Fibre Channel port group
FC LUN Masking	LUN masking is an authorization method that makes a LUN visible only to specified initiators. For details, see Masking a LUN from Fibre Channel initiators. **Note** This action is only available to Fibre Channel LUNs.
Edit LUN Settings	Edit the LUN settings.
Resize LUN	Resize the LUN capacity.
LUN Utilization	View LUN utilization percentages over a specified period of time.
Remove LUN	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.

LUN status

You can view LUN statuses by going to **iSCSI & Fibre Channel** > **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.

Status	Description
Disabled	The LUN is inactive and invisible to connected initiators.
[POOL_NAME] locked	The parent storage pool is locked. The LUN is inaccessible.
	The encrypted LUN is locked and inaccessible.
	The encrypted LUN is unlocked and accessible.

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 **Export LUN**.
   The **Create LUN Export Job** wizard opens.
3. 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 (_)
4. Select a storage pool.
5. Select a LUN.
6. Click **Next**.
7. 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.
8. Optional: Select **Enable 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.

9. Select the destination folder.

   Note
   To export to a remote folder, use HybridMount to mount the remote folder.

10. Click **Next**.
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. Review the summary information.
14. Click **Create**.

QuTS hero 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 **Import LUN**.
   The **Create LUN Import Job** wizard opens.
3. 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 (_)
4. Select the source image file.

   Note
   To import a file from a remote folder, use HybridMount to mount the remote folder.

5. Click **Next**.

6. Optional: Select **Enable deduplication on target LUN**.
   Deduplication reduces the amount of required storage space by eliminating duplicate copies of repeated data.
7. Select a target.

Option	Description
Overwrite an existing LUN	The imported LUN overwrites the selected existing LUN.
Create a new LUN	Creates a new LUN from the imported LUN image file. **a.** Select the destination storage pool. **b.** Specify a name for the LUN.

8. Click **Next**.
9. Review the summary information.
10. Click **Create**.

QuTS hero 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**. Identify a LUN import or export job, and then under **Action**, click ⋮ to select the desired action.

Action	Description
Edit Job	Edit the job.
Delete Job	Delete the job.
Start Job	Start the job.
Stop Job	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 status

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. LUNs are created from storage pool space.
   For more information, see Creating a block-based LUN.
3. Map the LUN to the iSCSI target.
   Multiple LUNs can be mapped to one target.
   For details, see Mapping a LUN to an iSCSI target.
4. Install an iSCSI initiator application or driver on the host.
   The host is the service, computer, or another 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**.
2. Click **Add Target**.
   The **Create iSCSI Target** wizard opens.
3. 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 (-)
4. Optional: Specify a different 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 ( )
5. 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.
6. Optional: Next to **Advanced Settings**, click ⌄ to configure advanced settings.

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. Optional: 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 CHAT authentication settings in **Protocol 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.

9. Click **Next**.
10. Select the IP addresses that this target will use for data transmission.
11. Click **Next**.
12. Specify which iSCSI initiators can connect to this target and perform read/write operations.

Option	User Action
Allow all iSCSI initiators	Enable **Allow all iSCSI initiators to connect and perform read/write operations**.
Allow only specified iSCSI initiators	**a.** Disable **Allow all iSCSI initiators to connect and perform read/write operations**. **b.** Click **Add Initiators**. **c.** Enter initiator IQNs, one per line. **d.** Click **Apply**.

13. Click **Next**.
14. Review the summary information.
15. Optional: Select **Map LUNs to target after target creation**.
16. Click **Create**.
    If you selected **Map LUNs to target after target creation**, the **Map LUNs to New iSCSI Target** window opens.
17. Map one or more LUNs to the new iSCSI target.
    This step is only available if you selected **Map LUNs to target after target creation**.

a. Select a mapping option.

- **Create a new LUN to map to target**
  After QuTS hero creates the iSCSI target, the **Create LUN** wizard opens.
- **Select LUNs to map to target**
  Select existing LUNs to map to the new target.

b. Click **Apply**.

QuTS hero creates the iSCSI target.

Editing iSCSI target settings

1. Go to **iSCSI & Fibre Channel** > **iSCSI**.
2. Identify an iSCSI target.
3. Click ⋮ > **Edit iSCSI Target**.
   The **Modify iSCSI Target** window opens.
4. Modify any of the following settings.

Setting	Description
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 ( )
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.
Advanced Settings	

Setting	Description
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. • **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.

CHAP authentication	When CHAP authentication is enabled, 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.
	• **No CHAP**: Do not use CHAP authentication for this target.
	• **Default CHAP**: Use the default CHAT authentication settings in **Protocol Settings** > **Default iSCSI CHAP** for this target.
	• **Customized CHAP**: Configure unique CHAP authentication settings for this target.
	  • Mutual CHAP forces both the initiator and target to authenticate each other.
	  • 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 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.

5. Click **Apply**.

QuTS hero saves the iSCSI target settings.

Binding an iSCSI target to an IP address

You can bind an iSCSI target to one or more IP addresses so that the iSCSI target can only be accessed via the IP addresses.

1. Go to **iSCSI & Fibre Channel** > **iSCSI Permissions**.
2. Identify an iSCSI target.
3. Click ⌄.
4. Go to the **Network Portal Binding** tab.
5. Optional: Select one or more IP addresses to bind to the iSCSI target.
6. Optional: Deselect one or more IP addresses to remove from the iSCSI target.
7. Click **Apply**.

QuTS hero applies the iSCSI target binding settings.

Mapping a LUN to an iSCSI target

Mapping a LUN to an iSCSI target allows an iSCSI initiator to connect to the LUN through the iSCSI target.

Note

Before you can map a LUN to a target, you must ensure the following:

- The LUN must be disabled.
  To disable a LUN, see LUN actions.
- If the LUN is encrypted, it must be unlocked.
  To unlock an encrypted LUN, see Managing LUN encryption.

1. Go to **iSCSI & Fibre Channel** > **LUNs**.
2. Identify a LUN.

   Tip

   Click **+** next to **Mapped LUNs** or **Unmapped LUNs** to view all LUNs in the group.

3. Under **Action**, click ⚙ > **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
4. Select **Map to new target**, and then select **iSCSI Target**.
5. Select an iSCSI target.

6. Optional: Enable the LUN.
   If the toggle switch is enabled, QuTS hero enables the LUN after mapping it to the target.
7. Click **Apply**.

QuTS hero saves the LUN mapping.

iSCSI target actions

You can perform various actions on iSCSI targets by going to **iSCSI & Fibre Channel** > **iSCSI**. Identify a target and perform one of the following actions.

Action	User Action	Description
Disable	Click  .	Disable an active target and disconnect all connected iSCSI initiators.
Enable	Click  .	Enable a deactivated target.
Edit	Click ⋮ > **Edit iSCSI Target**.	Edit the target's settings. For details, see Editing iSCSI target settings.
View connections	Click ⋮ > **View Connections**.	View the IP addresses and IQN information of all iSCSI initiators connected to this target.
Delete	Click ⋮ > **Delete iSCSI Target**.	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**.

Icon	Status	Description
🟢	Ready	The target is accepting connections but no initiators are currently connected.
🔵	Connected	An initiator is connected to the target.
⚫	Offline	The target is not accepting connections.

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 QuTS hero 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 Permissions**.
2. Click **iSCSI LUN ACL**.
   The **iSCSI LUN ACL** window opens.
3. Click **Add**.
   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 Permissions**.
2. Click **iSCSI LUN ACL**.
   The **iSCSI LUN ACL** window opens.
3. Identify a policy.
4. Under **Action**, click .
   The **Modify 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 Permissions**.
2. Click **iSCSI LUN ACL**.
   The **iSCSI LUN ACL** window opens.
3. Identify a policy.
4. Under **Action**, click .
   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, allowing connections from all iSCSI initiators.

Configuring an iSCSI target's authorized initiators list

1. Go to **iSCSI & Fibre Channel** > **iSCSI Permissions**.
2. Identify an iSCSI target.
3. Click ⌄ to expand the target.
4. Go to the **Initiator Access** tab.
5. Disable **Allow all iSCSI initiators to connect and perform read/write operations**.
6. Click **Add Initiators**.
   The **Add Initiators by Specifying IQNs** window opens.
7. Enter initiator IQNs, one per line.
8. Click **Apply**.
   The **Add Initiators by Specifying IQNs** window closes.
9. Optional: Click 🗑 to delete an initiator.
10. Click **Apply**.

Disabling iSCSI target authorization

Disabling iSCSI target authorization allows all iSCSI initiators to connect to the iSCSI target.

1. Go to **iSCSI & Fibre Channel** > **iSCSI Permissions**.
2. Identify an iSCSI target.
3. Click ⌄ to expand the target.
4. Go to the **Initiator Access** tab.
5. Enable **Allow all iSCSI initiators to connect and perform read/write operations**.
6. Click **Apply**.

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.

To use Fibre Channel service on your QNAP NAS device, you must first install a Fibre Channel card. You can find compatible cards at https://www.qnap.com/go/solution/fibrechannel-san.

Getting started with Fibre Channel

1. Install a Fibre Channel card on the NAS.
   - For the list of compatible QNAP Fibre Channel cards and NAS models, visit https://www.qnap.com/go/solution/fibrechannel-san.
   - For details on installing expansion cards, see the hardware user guide for your NAS model. You can download hardware user guides from https://www.qnap.com/go/download.
2. Create a Fibre Channel port group on the NAS.
   For details, see Creating a Fibre Channel port group.
3. Create a LUN on the NAS.
   A LUN is a portion of storage space. LUNs are created from storage pool space.
   For details, see Creating a block-based LUN.
4. Map the LUN to the Fibre Channel port group.
   For details, see Mapping a LUN to a Fibre Channel port group.
5. Install a Fibre Channel card on the host.
   The host is the service, computer, or another NAS device that will access the LUN.
6. Connect a Fibre Channel cable between the Fibre Channel ports on the host and the NAS.
7. Install a Fibre Channel initiator application or driver on the host.
8. Connect the Fibre Channel initiator on the host to the Fibre Channel port group on the NAS.

   Warning
   To prevent data corruption, multiple Fibre Channel initiators should not connect to the same LUN simultaneously.

   The LUNs mapped to the Fibre Channel port group appear as disks on the host.
9. In the host OS, format the disks.

Fibre Channel ports

You can view and configure the Fibre Channel ports on your Fibre Channel cards by going to **iSCSI & Fibre Channel** > **FC Permissions**.

Configuring Fibre Channel port binding

Port binding is a Fibre Channel security method that enables you to restrict which initiators are allowed to connect through a Fibre Channel port.

> **Tip**
> By default, port binding is disabled on all Fibre Channel ports, allowing any Fibre Channel initiator to connect.

1. Go to **iSCSI & Fibre Channel** > **FC Permissions**.
2. Identify a Fibre Channel port.
3. Click ⌄ to expand the port.
4. Click **Port Binding**.
5. Disable **Allow connections from all FC initiators**.
6. Add one or more initiator WWPNs to the port's authorized initiators list.
   For details on WWPNs, see Fibre Channel WWPNs.

Method	Steps
Add from WWPN list	**a.** Click **Add Initiators**, and then select **Add from WWPN Aliases List**. **b.** Select one or more initiator WWPNs in the WWPN list. **c.** Click **Add**.
Add WWPNs as text	**a.** Click **Add Initiators**, and then select **Input WWPNs Manually**. **b.** Specify one WWPN per line using the following format: `XX:XX:XX:XX:XX:XX:XX:XX` **c.** Optional: Select **Add new WWPNs to the FC WWPN Aliases List**. When selected, QuTS hero will add any unknown WWPNs to the list of known WWPNs. To view the list, go to **iSCSI & Fibre Channel** > **FC WWPNs**. **d.** Click **Add**.
Import from another FC port	**a.** Click **Add Initiators**, and then select **Import from Another FC Port**. **b.** Select a port. **c.** Click **Add**.

7. Click **Apply**.

QuTS hero applies the Fibre Channel port binding settings.

Fibre Channel port actions

You can perform various actions on Fibre Channel ports by going to **iSCSI & Fibre Channel** > **FC Permissions**. Click ⌄ to expand a port and then perform an action.

Action	Description
Edit alias	Click ✎ next to the alias to edit. The alias must consist of 1 to 20 characters. Valid characters include: letters (A-Z, a-z), numbers (0-9), hyphen (-), underscore (_)
Edit NPIV port WWPN	Click ✎ next to **NPIV** to open the **Edit NPIV Port** window. You can modify any of the last three bytes of the NPIV port WWPN. **Note** This action is only available when NPIV service is enabled. For details, see the following: • **Fibre Channel Service** in iSCSI & Fibre Channel global settings. • NPIV service for high-availability clusters
View connected initiators	Click **Connected Initiators** to see a list of all Fibre Channel initiators currently connected through the port.
Edit port binding	Click **Port Binding** to modify the port binding settings. Port binding allows you to define which initiators are allowed to connect through 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** > **FC Permissions**.

Icon	Status	Description
●	Online	The port has an active network connection.
●	Offline	The port does not have an active network connection.

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, QuTS hero 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 Channel port 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**.
2. Click **Add Port Group**.
   The **FC Port Groups** 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. Optional: Select **Map a LUN to the port group after this step**.
6. Click **Apply**.

QuTS hero creates the port group.

If you selected **Map a LUN to the port group after this step**, a LUN mapping window appears. You can select existing LUNs or create a new LUN to map to the new port group.

For details on creating a new LUN, see Creating a block-based LUN.

Mapping a LUN to a Fibre Channel port group

Mapping a LUN to a Fibre Channel port group allows a Fibre Channel initiator to connect to the LUN through the port group.

Note

Before you can map a LUN to a port group, you must ensure the following:

- The LUN must be disabled.
  For details, see LUN actions.
- If the LUN is encrypted, it must be unlocked.
  For details, see Managing LUN encryption.

1. Go to **iSCSI & Fibre Channel** > **LUNs**.

2. Identify a LUN.

   Tip
   Click **+** next to **Mapped LUNs** or **Unmapped LUNs** to view all LUNs in the group.

3. Under **Action**, click > **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.

4. Select **Map to a new target**, and then select **FC Port Groups**.

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 **Apply**.

8. Optional: Configure LUN masking.
   This step is only available if you selected **Keep LUN disabled and configure LUN masking in the next step**.

   a. Optional: Enable the LUN.
      If the toggle switch is enabled, QuTS hero enables the LUN after mapping it to the target.

   b. Disable **Allow connections from all FC initiators**.

   c. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	1. Click **Add Initiators**, and then select **Add from WWPN Aliases List**. 2. Select one or more initiator WWPNs in the WWPN list. 3. Click **Add**.

Method	Steps
Add WWPNs as text	1. Click **Add Initiators**, and then select **Input WWPNs Manually**. 2. Specify one WWPN per line using the following format: `XX:XX:XX:XX:XX:XX:XX:XX` 3. Optional: Select **Add new WWPNs to the FC WWPN Aliases List**. When selected, QuTS hero will add any unknown WWPNs to the list of known WWPNs. To view the list, go to **iSCSI & Fibre Channel** > **FC WWPNs**. 4. Click **Add**.

d. Click **Apply**.

QuTS hero saves the LUN mapping.

Fibre Channel port group actions

You can edit or delete Fibre Channel port groups by going to **iSCSI & Fibre Channel** > **Fibre Channel**.

Identify a port group, click ⋮, and then select one of the following actions.

Action	Description
Edit FC Port Group	Edit the name and member ports of the Fibre Channel port group.
Delete FC Port Group	Delete the Fibre Channel port group.

Fibre Channel LUN masking

LUN masking is a security feature that enables you to make a LUN visible to only specified Fibre Channel initiators. You can define the Fibre Channel initiators that can see a LUN by specifying the initiators' WWPNs.

For details on WWPNs, see Fibre Channel WWPNs.

> **Tip**
> By default, LUN masking is disabled for all Fibre Channel LUNs, allowing any Fibre Channel initiator to see them.

Masking a LUN from Fibre Channel initiators

1. Go to **iSCSI & Fibre Channel** > **LUNs**.

2. Identify a Fibre Channel LUN.

   Note
   The LUN must be disabled.
   To disable a LUN, see LUN actions.

3. Under **Action**, click  , and then select **FC LUN Masking**.
   \
   The **LUN Access Settings** window opens.

4. Disable **Allow connections from all FC initiators**.

5. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	**a.** Click **Add Initiators**, and then select **Add from WWPN Aliases List**. **b.** Select one or more initiator WWPNs in the WWPN list. **c.** Click **Add**.
Add WWPNs as text	**a.** Click **Add Initiators**, and then select **Input WWPNs Manually**. **b.** Specify one WWPN per line using the following format: `XX:XX:XX:XX:XX:XX:XX:XX` **c.** Optional: Select **Add new WWPNs to the FC WWPN Aliases List**. When selected, QuTS hero will add any unknown WWPNs to the list of known WWPNs. To view the list, go to **iSCSI & Fibre Channel** > **FC WWPNs**. **d.** Click **Add**.

6. Optional: Enable the LUN.

7. Click **Apply**.

QuTS hero applies the LUN masking settings.

Disabling Fibre Channel LUN masking

Disabling Fibre Channel LUN masking allows all Fibre Channel initiators to see the Fibre Channel LUN.

1. Go to **iSCSI & Fibre Channel** > **LUNs**.

2. Identify a Fibre Channel LUN.

   Note
   The LUN must be disabled.
   To disable a LUN, see LUN actions.

3. Under **Action**, click , and then select **FC LUN Masking**.
   The **LUN Access Settings** window opens.
4. Enable **Allow connections from all FC initiators**.
5. Optional: Enable the LUN.
6. Click **Apply**.

QuTS hero disables LUN masking and allows all Fibre Channel initiators to connect to the LUN.

Fibre Channel WWPNs

A WWPN (World Wide Port Name) is a unique identifier for a Fibre Channel port. A WWPN alias is a unique human-readable name for a Fibre Channel port that makes the port easier to identify.

You can manage WWPNs by going to **iSCSI & Fibre Channel** > **FC WWPNs**. The list automatically includes WWPNs for Fibre Channel ports on your NAS. You can perform the following actions:

Action	User Action
Add initiator WWPNs	1. Click **Add**. The **Input WWPNs Manually** window opens. 2. Specify one WWPN per line using the following format: `XX:XX:XX:XX:XX:XX:XX:XX` 3. Optional: Select **Add WWPNs of all logged-in FC initiators**. When selected, QuTS hero will add the WWPNs of all connected Fibre Channel initiators to the list. 4. Click **Add**. 5. Click **Apply**.
Remove initiator WWPNs	1. Select one or more initiator WWPNs. 2. Click **Remove**. 3. Click **Apply**.

<table>
<tr><th>Action</th><th>User Action</th></tr>
<tr><td>Edit a WWPN alias</td><td>
1. Identify a WWPN.
2. Under Alias, click to edit the WWPN alias field.
Note
• The alias can contain up to 20 characters. Valid characters include letters (A-Z, a-z), numbers (0-9), hyphen (-), and underscore (_).
• To remove the alias, clear the field.
3. Click outside the field to save changes.
4. Click Apply.
</td></tr>
<tr><td>Export WWPNs and aliases</td><td>Click Import/Export, and then select Export.
All WWPNs and WWPN aliases are exported as a CSV file. Each line in the file contains a WWPN, followed by a comma, and then the alias.</td></tr>
<tr><td>Import WWPNs and aliases</td><td>
1. Click Import/Export, and then select Import.
2. Locate and open a CSV file.
Each line in the file must start with a WWPN, followed by a comma, and then the alias. Example:
<pre>11:00:24:5e:be:00:00:06,Emulex1
11:00:f4:e9:d4:58:31:bd,QL16port1
10:00:00:99:99:99:99:87,Test1
10:00:00:99:99:99:99:89,Test2</pre>
3. Click Apply.
Note
• Identical aliases will be overwritten from the CSV file.
• Lines not formatted correctly will be ignored.
</td></tr>
</table>

NPIV service for high-availability clusters

iSCSI & Fibre Channel supports NPIV (N_Port ID Virtualization) service, which can help a high-availability (HA) cluster transfer Fibre Channel connections between node devices during failover or switchover.

To use Fibre Channel service in an HA cluster, the following conditions are required:

- NPIV service is enabled.

> **Note**
> When your device is part of an HA cluster, NPIV service is automatically enabled and cannot be disabled.
> For details on the NPIV service setting, see **Fibre Channel Service** in iSCSI & Fibre Channel global settings.

- The following conditions are identical between the two cluster nodes:
  - The same Fibre Channel card model is installed in the same PCIe slot on both nodes.
  - On both nodes, each corresponding connection uses the same Fibre Channel port on each node.
  - The Fibre Channel port used by each corresponding connection must be configured with the same NPIV port WWPN between the nodes.
    To edit a port's NPIV port WWPN, see Fibre Channel port actions.
  - Both nodes must be connected to a network switch that supports Fibre Channel and NPIV.

10. ZFS Pool Profiling Tool

ZFS Pool Profiling Tool controls the creation and execution of storage pool over-provisioning tests. These tests help determine the optimum amount of over-provisioning to set when creating a storage pool.

Installing ZFS Pool Profiling Tool

1. Log in to QuTS hero as an administrator.
2. Open **App Center**, and then click  .
   A search box appears.
3. Enter `ZFS Pool Profiling Tool`.
   The ZFS Pool Profiling Tool application appears in the search results.
4. Click **Install**.
   The installation window appears.
5. Click **OK**.

QuTS hero installs ZFS Pool Profiling Tool.

Storage pool over-provisioning

Over-provisioning reserves a specified percentage of space in a storage pool so that new data can be written into a complete block even if the pool is almost full. Higher pool over-provisioning provides higher write performance for intensive workloads and performance-demanding applications.

Creating a storage pool over-provisioning test

During a storage pool over-provisioning test, ZFS Pool Profiling Tool first fills the storage pool with random data. It then tests the random write performance of the storage pool 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%, ZFS Pool Profiling Tool will test pool write performance in five phases, with over-provisioning set to 0%, 5%, 10%, 15%, and 20%. If the random write performance of a disk is very low during any phase, ZFS Pool Profiling Tool will end the phase early and move to the next one.

1. Go to **ZFS Pool Profiling Tool** > **Review**.
2. Click **+ Create Test**.
   The **Create ZFS Pool 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 disk determines the optimum amount of over-provisioning for all disks of the same model and capacity. Selecting multiple disks 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.

   Important
   All selected disks must be of the same drive type (e.g., HDD, SSD).

   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
Over-provisioning test range	Specify the minimum and maximum amount of over-provisioning to test.
Test interval	Specify the over-provisioning increments to test.
End a test phase early if consistent performance is too low	ZFS Pool 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 disks, the test may take more than 24 hours.

   Tip
   If the estimated test time is too long, reduce the test range or test interval.

10. Click **Next**.
11. Verify the test information.
12. Click **Create**.
    A confirmation message appears.
13. Click **OK**.

ZFS Pool Profiling Tool creates and starts running the test. The test appears as a background task in QuTS hero.

Test reports

You can view, export, and delete test results in **ZFS Pool Profiling Tool** > **Test Reports**.

Icon	Description
	Open the report in a new window.
	Download a copy of the report in XLSX format.
	Delete the report.

Test reports provide the following information to help you determine the optimal amount of over-provisioning.

Section	Description
Test Information	View information about the NAS, the disks being tested, and the settings used in this test.
Test Result	View the test results as a graph. Choose from the following views: • IOPS / Time • IOPS / Data Written • Data Written / Time **Tip** Use these graphs to compare what effect different amounts of over-provisioning have on random write speeds (IOPS).

Section	Description
Over-Provisioning Evaluation Results	Enter an IOPS value in **Target write performance**. ZFS Pool Profiling Tool will recommend the amount of over-provisioning needed to consistently achieve the target random write performance.
Temperature	View the temperature of the disks during each test phase.
Test RAID Group	View information about the test pool RAID group. Details include the RAID type, number of disks, model and capacity of each disk, and disk read/write performance.

Settings

You can configure settings in **ZFS Pool Profiling Tool** >  > **Settings**.

Setting	Description
Maximum number of reports	ZFS Pool Profiling Tool retains the specified number of reports. Creating additional reports deletes the oldest ones.

11. Network & Virtual Switch

About Network & Virtual Switch

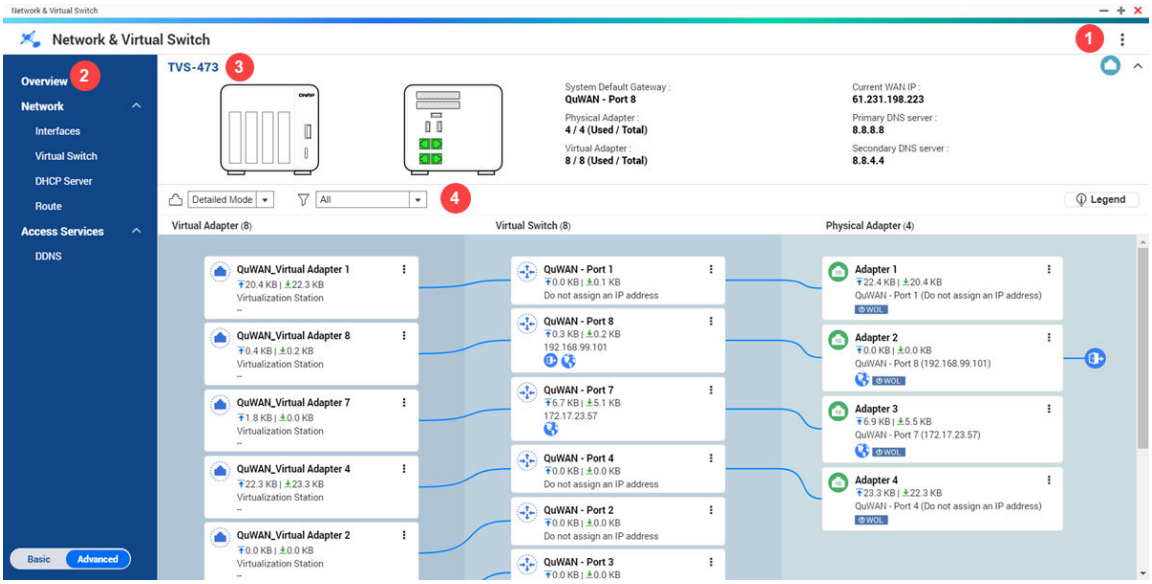
Network & Virtual Switch is a QuTS hero utility that provides a centralized interface for creating, configuring, and managing all network connections. It allows you to manage physical network interfaces, virtual adapters, Wi-Fi, and Thunderbolt connections, as well as control network services such as DHCP, DDNS, and default gateways.

Important

If high availability (HA) is enabled, both nodes must have matching network interfaces. If the passive node does not have the required interface, configuration changes for the system default gateway, port trunking, VLAN, virtual switch, or static routes will fail. When the passive node is disconnected, removed, or in a split-brain state, only deletion operations are allowed. Add and edit operations are disabled, except for interface configuration and virtual switch IP settings.

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.

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 QuTS hero 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**.

Note

Network & Virtual Switch supports hot-pluggable network adapters such as E1.S NICs. When a removable adapter is unplugged, its interface remains visible in the list with a trash can icon, indicating that the configuration is retained temporarily.

- Related virtual switch, VLAN, port trunking, static route, and system default gateway settings are preserved but hidden while the adapter is disconnected.
- DHCP server settings configured on the adapter are automatically cleared. If the adapter is reinserted, the original settings (except DHCP server) are restored automatically, even if the adapter is installed in a different slot.
- Clicking  permanently removes all configurations related to the disconnected adapter.

Configuring IPv4 settings

1. Log on to QuTS hero 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.
5. Click > **Configure**.
   The **Configure** window opens.
6. Click **IPv4**.
7. Configure the IPv4 settings.
   a. Click **Enable IPv4 settings**.
   b. Optional: Select **DHCP IP** to allow the DHCP server on the network to automatically assign the necessary network configurations to the device.
   c. Optional: Select **Static IP** to manually assign the following IP information.
      - Fixed IP address
      - Subnet mask
      - Default gateway
   d. Optional: 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. QuTS hero 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.

e. Optional: 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.

8. Click **Apply**.

Network & Virtual Switch updates the IPv4 settings.

Configuring IPv6 settings

1. Log on to QuTS hero 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.
5. Click ⋮ > **Configure**.
   The **Configure** window opens.
6. Click **IPv6**.
7. Click **Enable IPv6 settings**.
8. Select an IPv6 setting.
   - **Stateful Address Autoconfiguration**: Automatically configures the IPv6 address, prefix length, default gateway, and DNS server settings using information provided by a DHCPv6 server.

- **Stateless Address Autoconfiguration**: Automatically configures the IPv6 address and default gateway based on router advertisements.
  Optional: Click **Generate a SLAAC address with a secret key** to create a randomized, privacy-enhanced IPv6 address.
- **Use static IP address**: Manually configure the following IPv6 information.
  - Fixed IP address
  - Prefix length
  - Default gateway

9. 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 QuTS hero 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	QuTS hero utilizes a dynamic algorithm to analyze network interfaces and automatically designate the most suitable option as the primary route for external communication.

Setting	User Action
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, QuTS hero 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 QuTS hero 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 QuTS hero 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. Click **IPv4** or **IPv6**.

   Note
   Starting from QTS 5.2.5 and QuTS hero h5.2.5, DNS server settings for IPv4 and IPv6 are configured separately. In earlier versions, both protocols were configured together on a single interface. Verify your firmware version and configure the appropriate settings for your network environment.

5. Scroll down to **DNS server connection**.
6. Select one of the following options:
   - **Automatic**: Automatically obtain the IP address using DHCP.
   - **Manual**: 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. If your network uses both IPv4 and IPv6, ensure you configure DNS server addresses for both protocols if your firmware version supports separate configurations.

7. 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 **Add DHCP Server** window opens.

4. Select an interface.

   Important
   You can now create a DHCP server even when the adapter is assigned a DHCP IP address. However, it is strongly recommended to use a static IP address to ensure consistent network behavior.

5. Click **Next**.
6. Configure the basic DHCP server settings.
   a. Optional: Click  next to the IP address to change the existing IP address.
   The **Edit IP Settings** window appears.
   b. Specify a fixed IPv4 address.
   c. Select the subnet mask from the drop-down menu.
   d. Specify the default gateway IP address.
   e. Select the jumbo frame to improve network performance when transferring large amounts of data.
   f. Select the appropriate network speed to match your network infrastructure.
   g. Optional: Specify the primary and secondary DNS server IP addresses.
   h. Click **Apply**.
   The **Edit IP Settings** window closes.
7. Specify the starting IP address.
8. Specify the ending IP address.
9. Select the subnet mask from the drop-down menu.
10. Set the lease time for leased IP addresses.
11. Select a default gateway.
    - **Interface IP address**: Select to set the default gateway IP address to match the interface IP address configured as the DHCP server.
    - **Manual IP**: Select to manually enter the default gateway IP address for the DHCP server.
12. Optional: Specify the primary and secondary DNS server IP addresses.
13. Optional: Configure the advanced DHCP server settings.
    a. Click **Advanced Settings**.
    Network & Virtual Switch displays the advanced DHCP server settings.
    b. Enter the IP address of the WINS server to support NetBIOS name resolution.
    c. Specify the domain name to assign to DHCP clients.

d. Enter the IP address of the TFTP server for clients to download boot files or configuration files.

e. Specify the boot file name that DHCP clients will download from the TFTP server during network boot.

14. Add clients and reserve IP addresses.

a. Click **Clients and Reserved IPs**.

b. Click **Add**.
The **Add Reserved IP** window appears.

c. Enter the device name.

d. Specify the IP address to reserve the IP address for the device.

e. Specify the MAC address of the device.

f. Click **Apply**.
The IP reservation window closes.

Tip

To unreserve one or more IP addresses, go to the **DHCP Server** page and click **Add** or under **Actions** for an existing DHCP server. Click **Clients and Reserved IPs**, select the IP addresses you want to unreserve, click **Unreserve**, and then click **Apply**.

15. Click **Apply**.

Network & Virtual Switch adds the DHCP server.

Note

- When editing DHCP server settings, the interface IP address cannot be modified.
- The **Enable DHCP Server** option can be configured during the edit process but is not available when creating a new DHCP server.
- You can assign the current DHCP IP address of a client device as a reserved IP address to ensure it always receives the same address from 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.
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 QuTS hero 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.

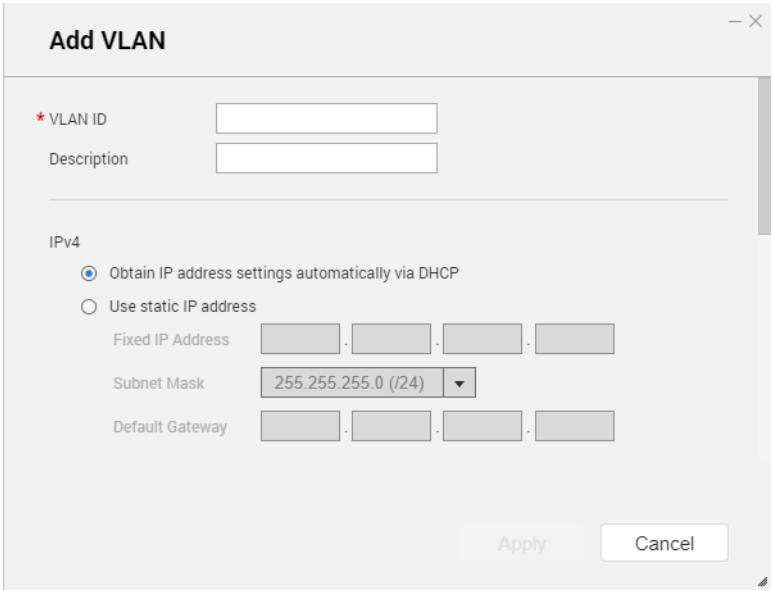
Configuring VLAN settings

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**.
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.

Important
If you set a virtual switch as the cluster interface in High Availability Manager, the cluster IP (CIP) is automatically displayed in Network & Virtual Switch. When a CIP is present, you cannot change any IPv4 network settings. You can only modify the IPv6 settings, and the virtual switch cannot be deleted.

QuTS hero 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.
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 to prevent bridge loops**.

   Tip
   Enabling this setting prevents bridge loops.
7. Click **Next**.
8. Configure a MAC address for the virtual switch.
   - **Automatically assign a MAC address**: Generate and assign a MAC address automatically.
   - **Select a MAC address from a physical adapter**: Use the MAC address of a selected physical adapter.
   - **Enter or generate a random MAC address**: Enter a custom address or generate one randomly by clicking **Generate MAC Address**.

   Note
   Network & Virtual Switch automatically uses the MAC address of the selected physical network adapter.
9. Click **Next**.
10. Configure the virtual switch IP address settings.
    a. Select **Enable IPv4 settings**.

Connection Type	Description
DHCP Client	Assigns a dynamic IP address to the virtual switch.

Connection Type	Description
Static IP	Assigns a static IP address to the virtual switch. • **Use the same settings as the selected adapter**: Inherits the IP configuration from the connected physical adapter. • **Manually configure the IP address**: Allows you to set a custom static IP configuration for 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.

b. Next to **DNS server connection**, select one of the following.

- **Automatic**: Obtains DNS server information automatically from the network.
- **Manual**: Allows you to specify the primary and secondary DNS server addresses manually.

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 primary DNS server address for the DHCP server.

g. Optional: Specify a secondary DNS server address 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**
> QuTS hero supports both PXE and remote booting of devices.

k. Specify location and file name of the TFTP server boot file.

> **Tip**
> QuTS hero supports both PXE and remote booting of devices.

14. Click **Next**.

15. Configure the virtual switch IPv6 address.

a. Select **Enable IPv6 settings**.

b. Select the connection type.

- **Stateful Address Autoconfiguration**: 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.

- **Stateless Address Autoconfiguration**: The adapter automatically acquires an IPv6 address and DNS settings from the router.
  Optional: Enable **Generate a SLAAC address with a secret key** to create the IPv6 address using a secret key to add privacy and prevent tracking based on the adapter's hardware address.

  > **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)
  - Gateway (Specify a default gateway prefix between FE80 and FEB)

c. Next to **DNS server connection**, select one of the following.

- **Automatic**: Obtains DNS server information automatically from the network.
- **Manual**: Allows you to specify the primary and secondary DNS server addresses manually.

16. Click **Next**.

17. Confirm the virtual switch settings.

18. 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 QuTS hero 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 QuTS hero 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**.
- QuTS hero 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 QuTS hero 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
Authentication	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.
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** QuTS hero 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.

Setting	User Action
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

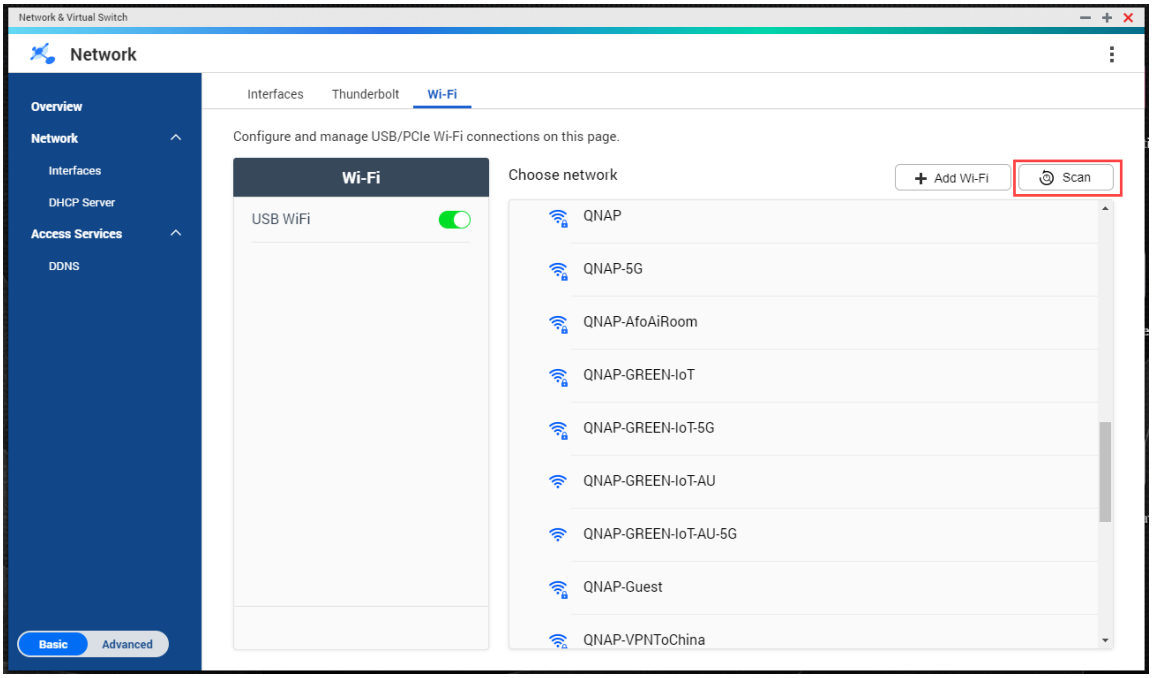
A captive portal allows organizations to easily share their network environment with customers, employees, and other guests.

QuTS hero 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.

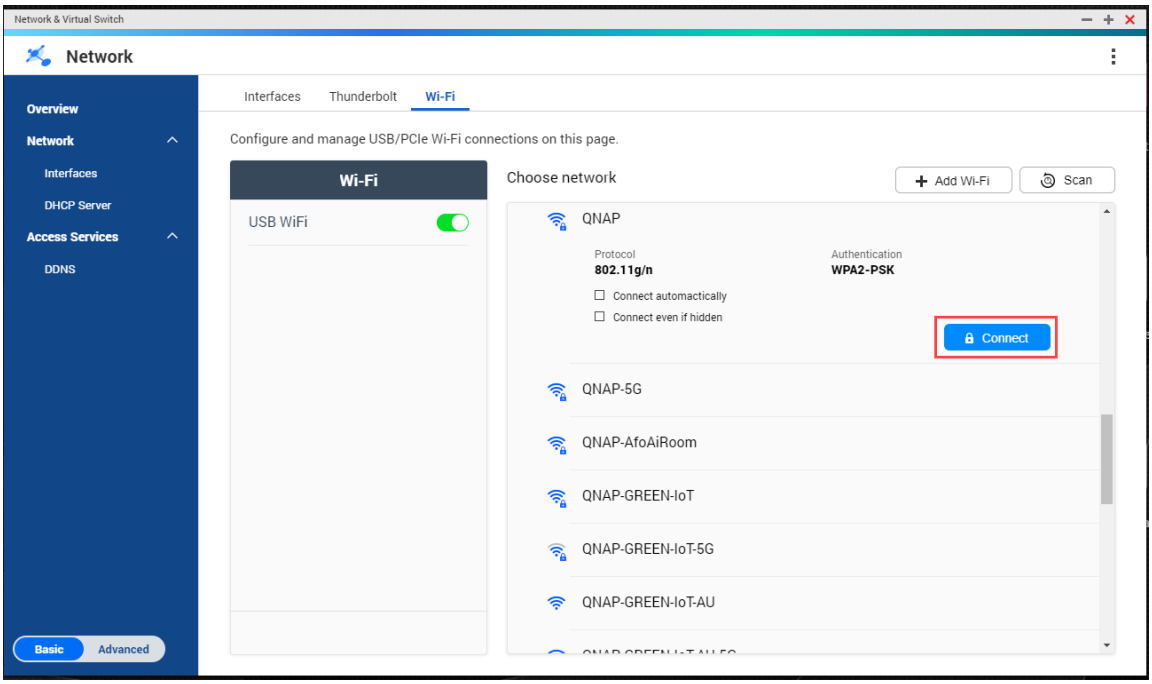
1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces**.
3. Go to the **Wi-Fi** tab.

4. Optional: Click **Scan** to search for accessible wireless networks with a captive portal.

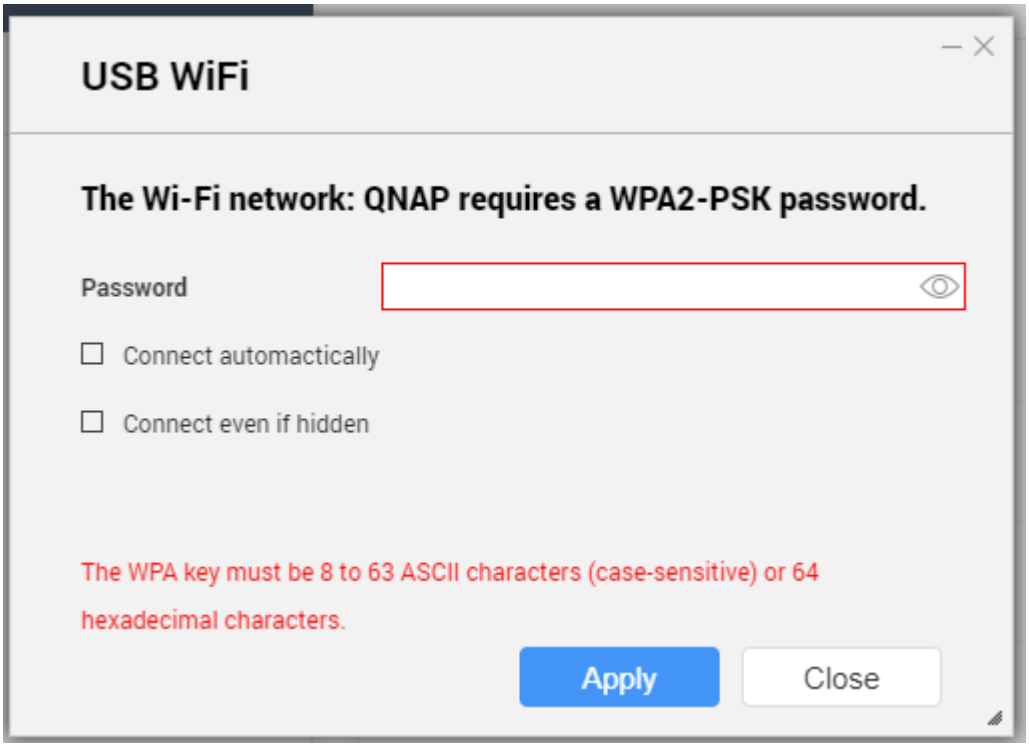


5. Select the captive-portal-enabled wireless network from the list.
The settings panel expands.

6. Click **Connect**.

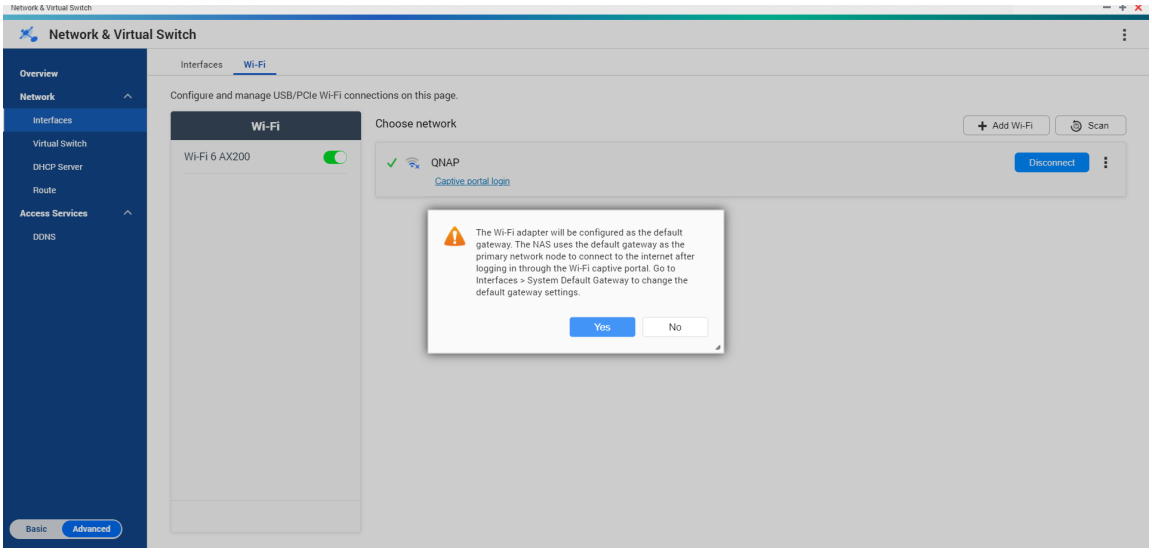


7. Optional: Configure connection settings.



For configuration details and wireless icon descriptions, see Connecting to a wireless network.

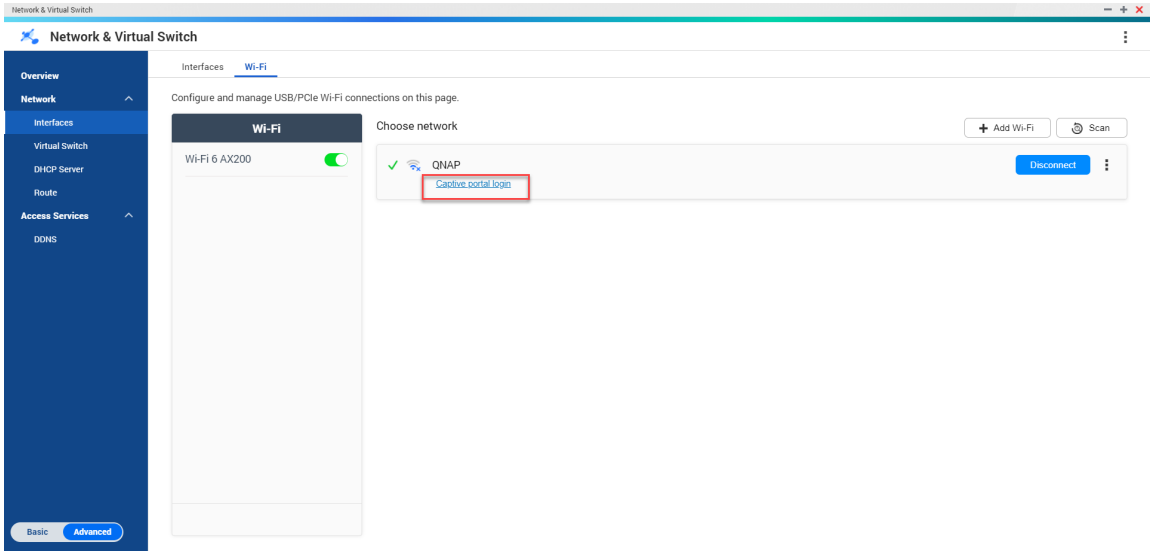
8. Click **Apply**.
A popup window opens specifying the change in the default network gateway.



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.
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 QuTS hero 5.0.0. To install the application, go to **App Center** > **All Apps**, and then install the WirelessAP Station application.

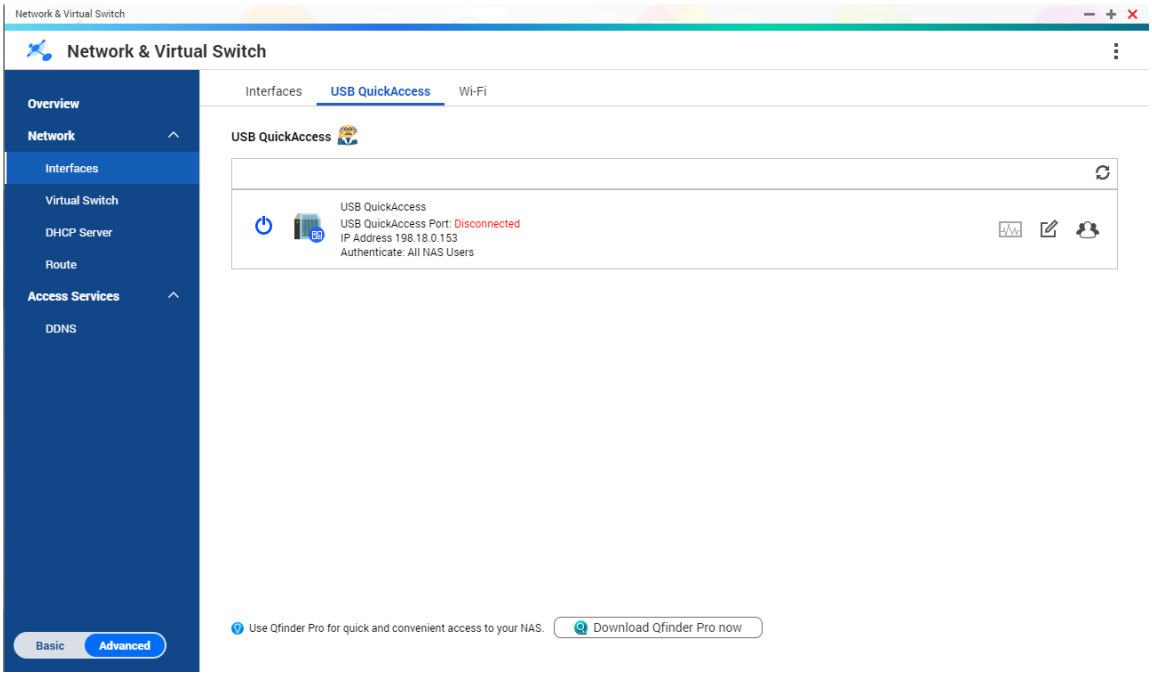
1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch**.
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces**.
3. Click the **WirelessAP Station** tab.

QuTS hero 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 QuTS hero username and password is required to access files.
Everyone	No username or password is required to access files.

Authentication Method	Description
Selected Users/ Groups	Administrators can grant access to specific QuTS hero users or groups. A QuTS hero 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.

Note
QuTS hero h6.x supports Thunderbolt 5 connectivity.

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.
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 QuTS hero interface.

Note

QNAP recommends keeping the expansion card firmware up-to-date. By default, QuTS hero 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**.
   QuTS hero starts updating the network expansion card firmware.
   After the firmware is updated, a restart confirmation window appears.
4. Click **Restart**.

QuTS hero restarts the device to apply the network expansion card firmware changes.

12. Network & File Services

About Network & File Services

The Network & File Services utility allows QuTS hero 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

QuTS hero 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, QuTS hero 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, QuTS hero 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 QuTS hero 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 QuTS hero 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 QuTS hero 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 QuTS hero.
SNMP Trap Level	Select the type of alert messages that the NAS will send to the NMS. • **Information**: QuTS hero sends information regarding ongoing or scheduled NAS operations. • **Warning**: QuTS hero sends alerts when NAS resources are critically low or the hardware behaves abnormally. • **Error**: QuTS hero 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** and specify a privacy password containing 8 to 64 ASCII characters.

5. Click **Apply**.

QuTS hero 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 1.3.6.1.4.1.55062.

1. Go to **Control Panel** > **Network & File Services** > **SNMP**.
2. Under **SNMP MIB**, click **Download**.
   QuTS hero 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. Click **Manage SMB Service Settings**.
   QuTS hero opens the SMB Service application and redirects you to the **General** tab in the **SMB Service Settings** page.

3. Enable **SMB Service**.
4. Configure the general settings.
   a. Specify the workgroup name and description.

Setting	User Action
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: ~ ! @ # $ ^ & ( ) - _ { } . '
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.

   b. Click **Apply**.
   SMB Service saves the general settings.
5. Click **Advanced**.
   The **Advanced** window opens.
6. Configure the SMB server protocol settings.
   a. 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.

   b. 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.

   c. Enable **Allow NTLMv2 authentication only** to authenticate clients using only NT LAN Manager Security Support Provider.
   When this option is deselected, QuTS hero uses NT LAN Manager (NTLM).

d. 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.

e. 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.

f. Under **Restrict anonymous users from accessing SMB shared folders**, select one of the following to enable user login before accessing SMB shared folders..

- **Enable (strict)**: Requires all users to authenticate before accessing any SMB shared folders. Anonymous access is completely blocked.
- **Enabled**: Allows limited guest access, but users must still provide valid credentials to access most SMB shared folders.
- **Disabled**: Permits anonymous users to access SMB shared folders without authentication. Use this option only in trusted or isolated network environments.

g. Select a server signing option to secure message transmissions and prevent relay attacks.

- **Sign if client agrees**: The server signs SMB messages only if the client also supports and requests signing. This provides basic protection while maintaining compatibility with older clients.
- **Enforce signing**: The server requires all SMB message transmissions to be signed. Clients that do not support signing will be denied access. This ensures maximum security against relay and tampering attacks.
- **Sign according to selected SMB version**: The server applies message signing rules based on the configured SMB protocol version. Signing behavior follows the version-specific security policies (for example, SMB 3.0 and later always enforce signing).

7. Configure SMB server performance settings.

a. Select **Enable Asynchronous I/O** to improve the Samba performance using asynchronous I/O.

b. Select **Accelerate file transfer using kernel SMB daemon** to boost SMB performance and reduce latency.
Optional: Select **Accelerate copying large number of small files** to improve transfer speed and efficiency when handling many small files.

8. Configure SMB server name resolution settings.

   a. Select **Enable WINS server** to run a WINS server on the NAS.

      - **Automatically use the Samba WINS server:** The device automatically uses its built-in Samba WINS service for name resolution.
      - **Manually enter a WINS server IP address:** Specify the IP address of an external WINS server for network name resolution.

   b. Select the name resolution priority to define the order used for resolving network hostnames.

      - **Try WINS then DNS:** The system attempts to resolve names using the WINS server first, then falls back to DNS if not found.
      - **Try DNS then WINS:** The system resolves names using DNS first, and uses WINS only if the DNS query fails.

   c. Enable **Local master browser** to allow the device to manage and maintain the list of all devices on the local network for easier network browsing.

   d. Enable **Enable WS-Discovery to help SMB clients discover the NAS**to allow clients to find the NAS more easily on the local network without specifying its IP address.

9. Configure additional settings.

   Note
   DNS settings are available only when Active Directory (AD) authentication is activated.

   a. Enable**Automatically register in DNS** to allow the device to automatically update its DNS records in the Active Directory domain.

   b. Select **Enable trusted domains** to allow users from trusted external domains to access the NAS using their domain credentials.

      Note
      When this option is disabled, the SMB Service no longer sends any trusted domain protocol requests. User and group information from trusted domains will not appear in Control Panel.

   c. Enable **Alternative login style (Domain/USERNAME)** to let users log in using the format `Domain/Username` instead of the default `Username@Domain` style.

   d. 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.

e. Specify the veto criteria for hiding files from SMB NAS users.

> **Note**
> This option is only available when **Veto files** is selected.

10. Click **Apply**.

Network & File Services saves the Samba settings.

Configuring network binding and SMB multichannel settings

You can configure network binding and SMB Multichannel settings in the SMB Service application. SMB Service is a standalone application that provides options to configure and manage SMB settings, including service behavior, network performance, and access permissions.

1. Open SMB Service.
   The **Overview** page appears.
2. Configure network binding settings.
   Network binding defines and controls which network interfaces SMB can use for data transmission, allowing you to manage and isolate SMB traffic across specific interfaces.
   a. Go to **SMB Service** > **Network Settings** > **Network Binding**.
   b. Select one of the following.
      - **All network interfaces**: Allows SMB to use all available network interfaces on the NAS for data transmission.
      - **Only selected network interfaces**: Limits SMB traffic to the specified network interfaces only.

      > **Note**
      > When high availability (HA) mode is enabled, this option is disabled to prevent the heartbeat network interface from being included in the binding list.

   c. Click **Apply**.
      SMB Service applies the selected network binding setting.
3. Configure the SMB multichannel settings.
   SMB multichannel enables SMB to establish multiple simultaneous network connections, improving transfer performance and providing higher fault tolerance.
   a. Go to **SMB Service** > **Network Settings** > **SMB Multichannel**.
   b. Select **Enable SMB Multichannel**.
   c. Select one of the following.
      - **Automatic**: Allow the system to automatically select multiple network adapters that possess similar configurations.

- **Manual**: Manually choose two or more network adapters that have the same network speed.

d. Click **Apply**.
SMB Service saves the SMB multichannel 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.

Permission	Status	Description
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	Enabled	**read-only**: Allows NFS clients to view and read files and directories in the shared folder but prevents them from modifying, renaming, or deleting content.
		read/write: Allows NFS clients to view, create, modify, and delete files and directories in the shared folder.
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. Select **NFS over RDMA (high-speed data transfer)**.

   Note

   - Remote Direct Memory Access (RDMA) allows direct data exchange between the NAS and client memory, reducing CPU load and latency while improving transfer performance.
   - This option is available only when the NAS is equipped with RDMA-capable network adapters, such as the QXG-100G2SF-BCM or the NVIDIA® ConnectX®-6 Dx.

   d. Optional: Click **Advanced Options**.

   e. 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 QuTS hero 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 QuTS hero 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 QuTS hero 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**.
   QuTS hero 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 **Edit Properties**.
   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**.

13. 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**.

Installing an SSL certificate

Important
myQNAPcloud SSL certificate 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 certificate	The myQNAPcloud SSL certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users. This certificate is provided and maintained by QNAP and is available for long-term support.	• Click **Buy Now** if you have not yet purchased a myQNAPcloud SSL certificate. Follow the on-screen instructions to complete the purchase and installation. • Click **Install** if you have already purchased a myQNAPcloud SSL certificate and have not yet installed the certificate. This allows you to choose a purchased certificate to install. For more details on how to purchase, install, and manage a myQNAPcloud SSL certificate, see the following tutorials. • How to purchase and install a myQNAPcloud SSL certificate? • How to extend and renew a myQNAPcloud SSL certificate?

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 its limitations. We recommend choosing a myQNAPcloud SSL certificate for ease of use.	**a.** Click **Install 90-day SSL**. 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**.

14. App Center

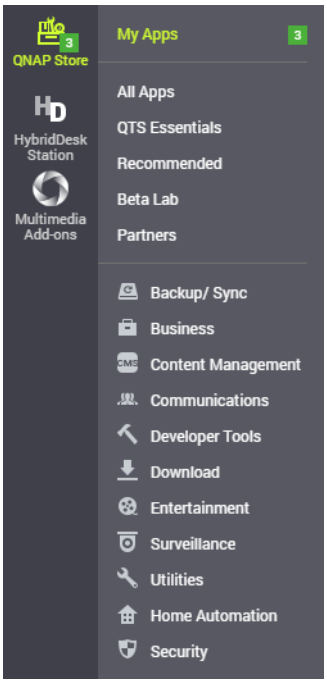
App Center is a digital distribution and management platform in QuTS hero where you can browse, download, and manage applications and utilities developed for the QNAP NAS.

Navigation

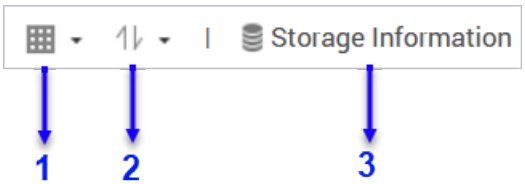
You can view all App Center apps in the left panel or configure a number of settings using the toolbar.

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

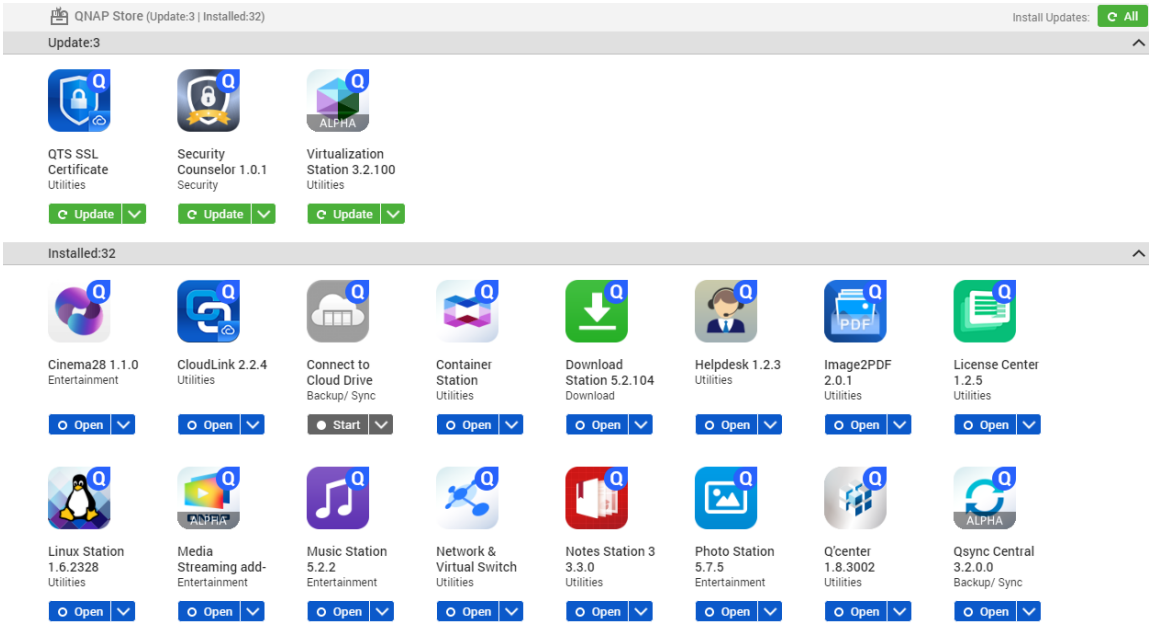
No.	Elements	Possible User Actions
1	View mode	• Click the icon to switch between two view modes. • Click ˇ and select a view mode.
2	App sorting	Click ˇ and select an app sorting method.
3	Storage information	View the basic storage pool information and the installation locations of your apps. For more storage pool 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.

Main area

The main area allows you to browse available apps and manage your installed apps. For details, see App management.



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 storage pool to better allocate system resources. Certain apps, however, must be installed on the system storage pool 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 storage pool.
6. Click **Migrate**.
   A confirmation message appears.
7. Click **OK**.

Granting or denying user access to an app

QuTS hero 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, QuTS hero 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	QuTS hero 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.
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**.

15. 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 QuTS hero 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 on QuTS Hero**.
    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 on QuTS Hero**.
    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.

16. Multimedia

QuTS hero provides a range of applications and utilities for viewing, playing, and streaming multimedia files stored on the NAS.

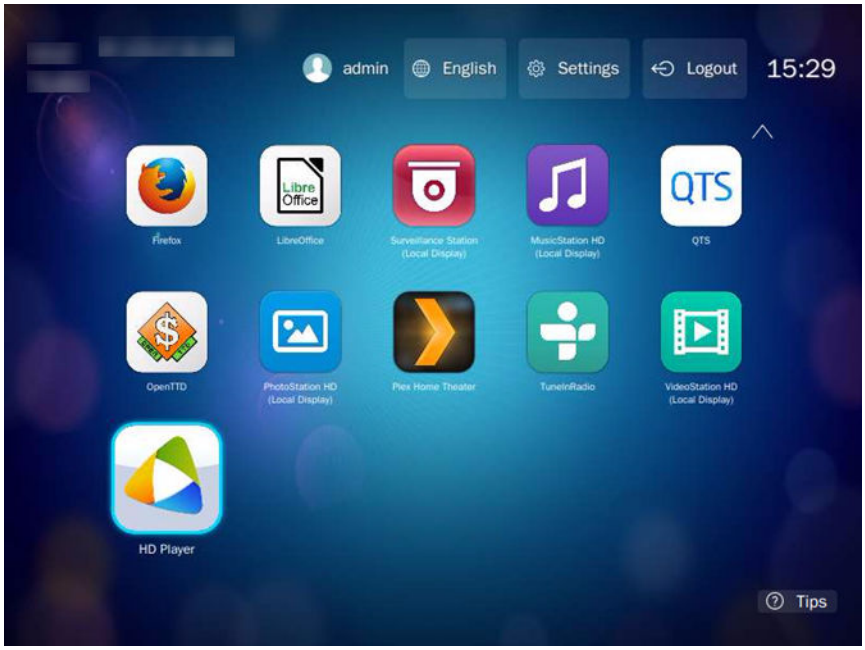
Application/Utility	Description
HybridDesk Station (HD Station)	Connect to an HDMI display to access multimedia content on your NAS.
DLNA Media Server	Configure your NAS as a Digital Living Network Alliance (DLNA) server to access media files on your NAS from devices on your home network.
Media Streaming 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**.

QuTS hero 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.

DLNA Media Server

You can configure your NAS as a Digital Living Network Alliance (DLNA) server, allowing you to access media files on your NAS through your home network using DLNA devices such as TVs, smartphones, and computers.

The contents displayed in DLNA Media Server are based on user account permissions and Multimedia Console settings.

Important

- You must enable Multimedia Services before using DLNA Media Server. Go to **Control Panel** > **Applications** > **Multimedia Console** > **Overview** to enable Multimedia Services.
- The first time you enable DLNA Media Server, QuTS hero automatically installs the Media Streaming Add-on if it is not already installed on the NAS. For details, see Media Streaming Add-on.

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.

Configuring DLNA Media Server

1. Go to **Control Panel** > **App Center**.
2. Open **Media Streaming add-on**.
3. 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 QuTS hero multimedia applications:

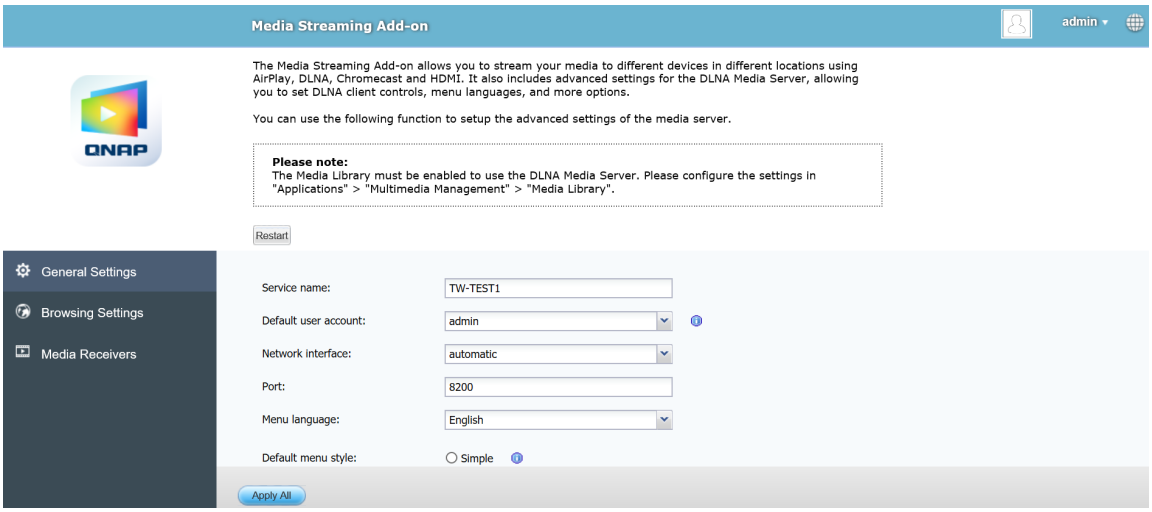
- File Station
- Photo Station
- Music Station

- 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 QuTS hero 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.

Setting	Description
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 QuTS hero 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 QuTS hero 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.

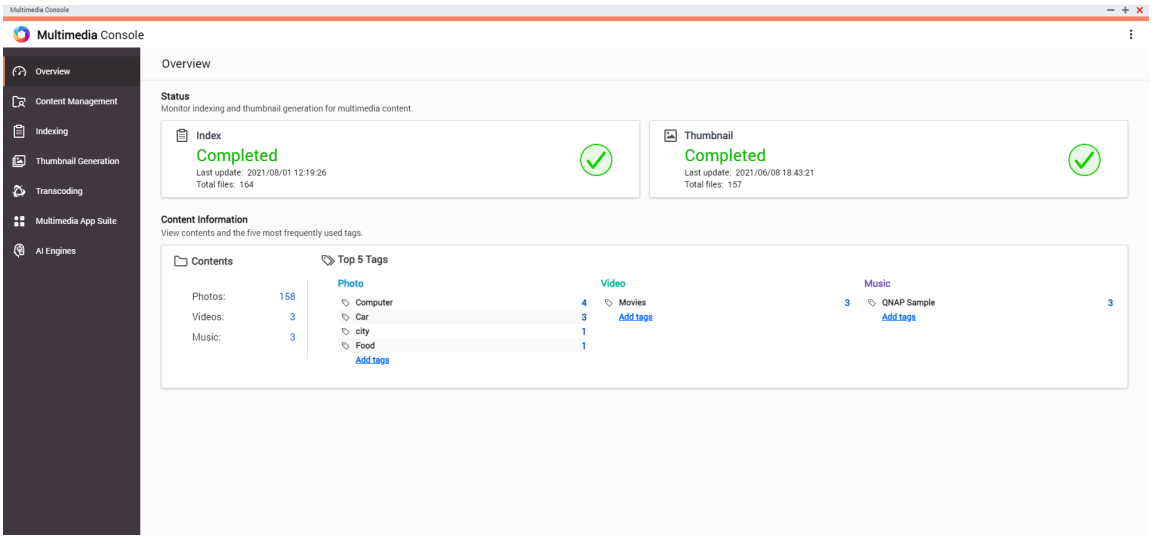
4. Click **Apply All**.

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.

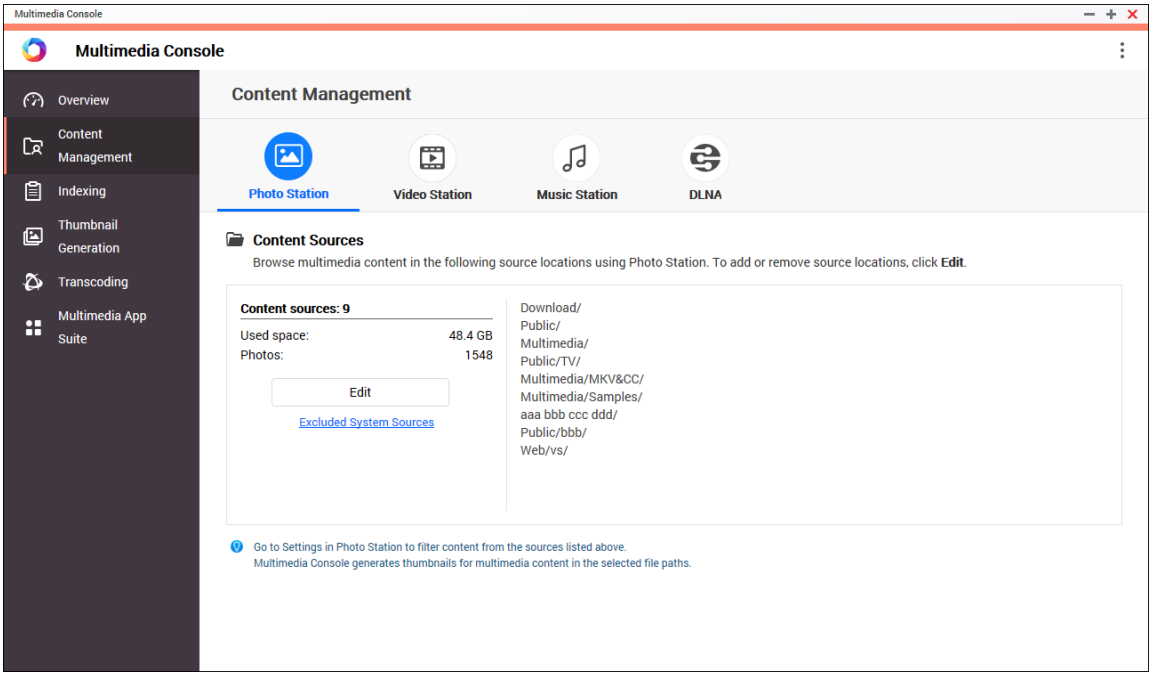
Overview

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



Content Management

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.



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.

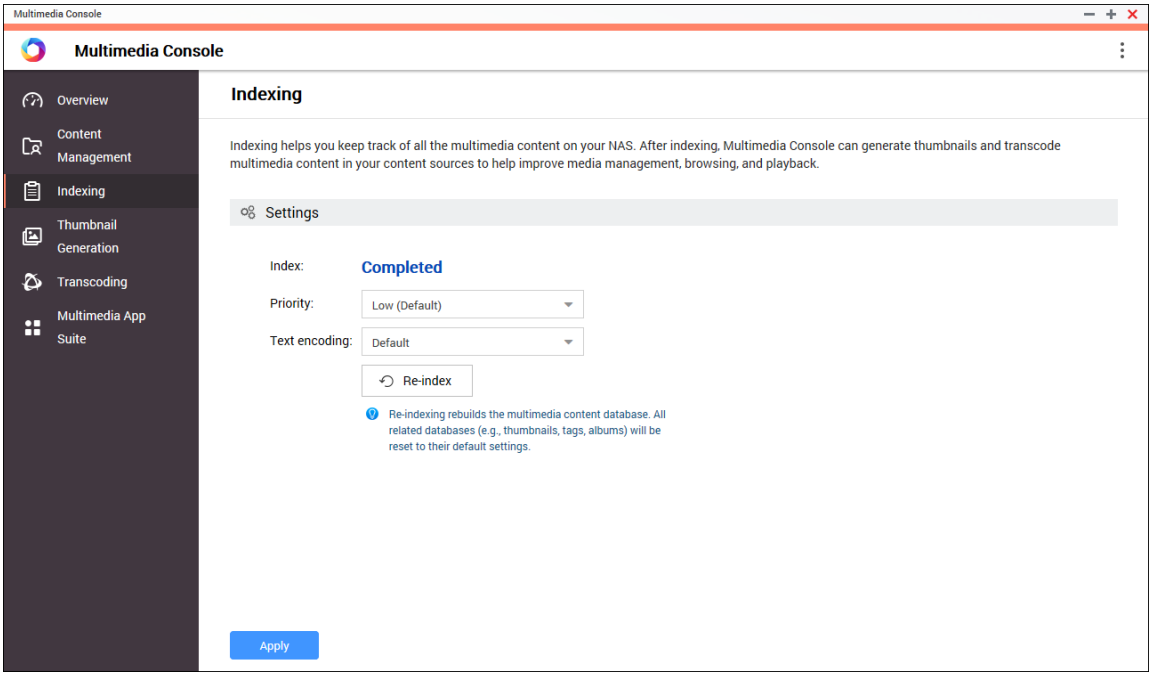
1. Open Multimedia Console.

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 Console improves content management, browsing, and playback when accessing files in various multimedia apps by scanning and indexing multimedia files on your NAS.



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 Media Viewer to be installed, and may also require a CAYIN Media Viewer 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.

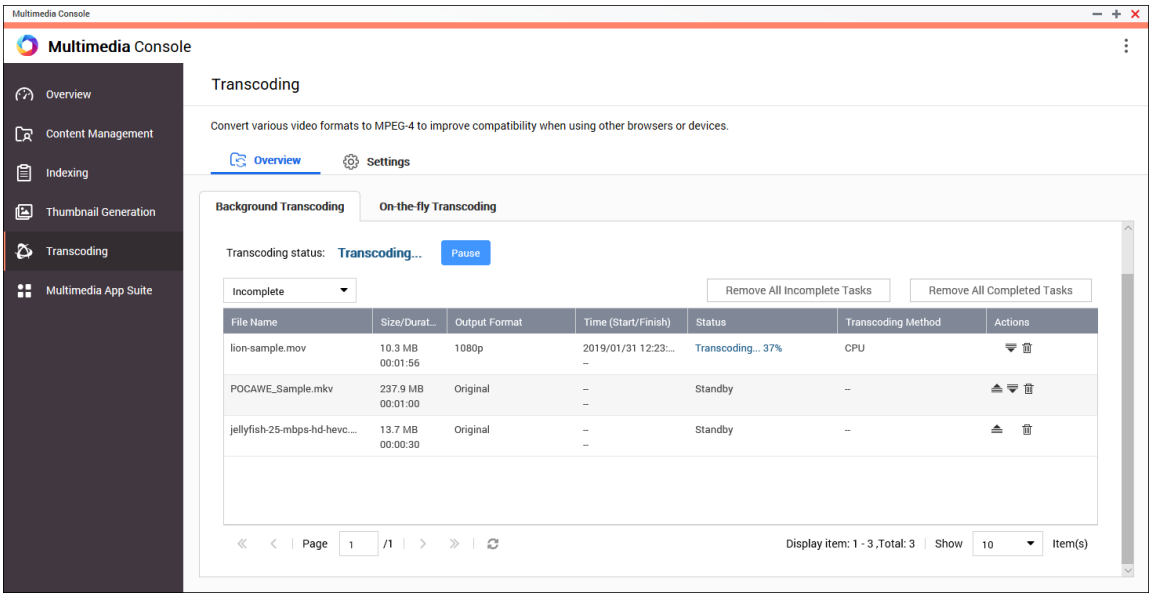
Note

- 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.

Background Transcoding

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.



General Tasks

Task	User Action
Pause background transcoding	1. Click **Pause**. The **Pause** window opens. 2. Select **Pause**. 3. Click **OK**. **Tip** Click **Resume** when background transcoding is paused to resume background transcoding.

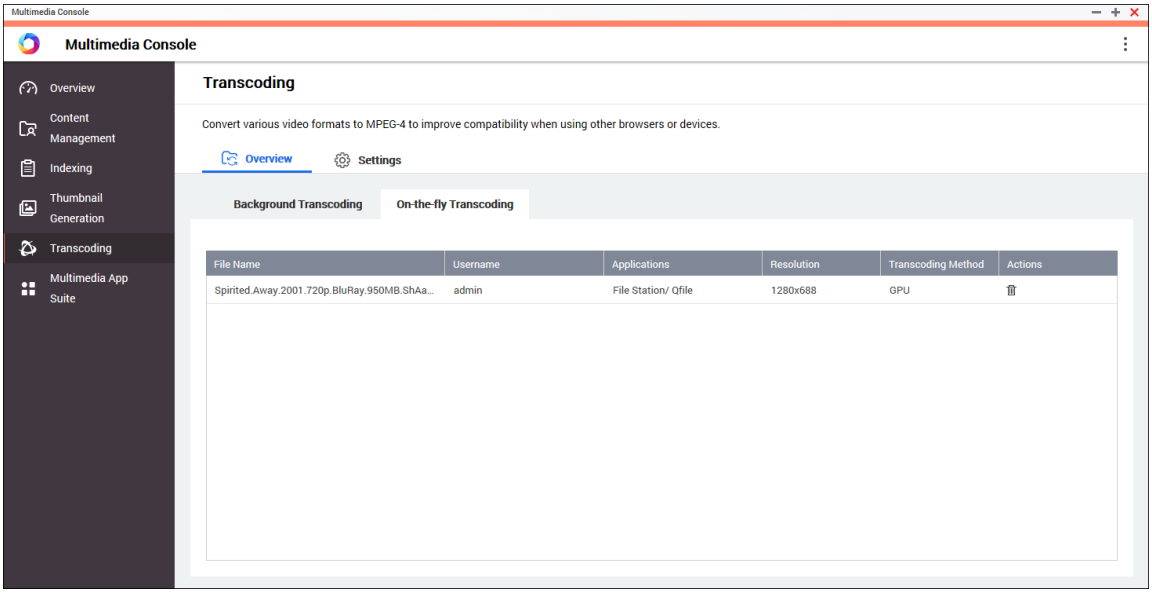
Task	User Action
Postpone background transcoding	1. Click **Pause**. The **Pause** window opens. 2. Select **Postpone**. a. Select the duration. 3. Click **OK**. **Tip** Click **Resume** when background transcoding is postponed to resume background transcoding.
View completed tasks	Above the background transcoding task table, select **Completed** from the drop-down list. Multimedia Console displays completed background transcoding tasks.
View incomplete tasks	Above the background transcoding task table, select **Incomplete** from the drop-down list. Multimedia Console displays incomplete background transcoding tasks.
Remove incomplete tasks	1. Click **Remove All Incomplete Tasks**. A dialog box appears. 2. Click **OK**.
Remove completed tasks	1. Click **Remove All Completed Tasks**. A dialog box appears. 2. Click **OK**.

Task Table Configuration (Incomplete Tasks)

Button	Description
	Moves a task up in the list and increases its priority.
	Moves a task down in the list and decreases its priority.
	Removes a task from the list.

On-the-fly Transcoding

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.

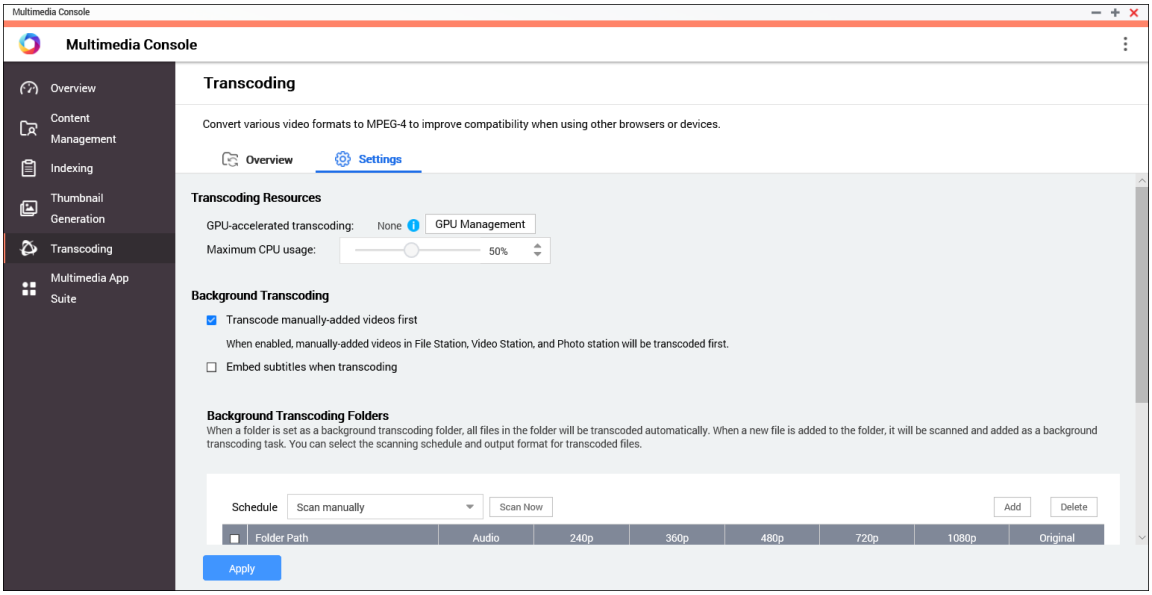


Tip

Click 🗑 to remove a task from the list.

Settings

You can manage Background Transcoding and On-the-Fly Transcoding settings from the Settings tab on the **Transcoding** screen.



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.

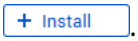
Task	User Action
Configure the scanning schedule for background transcoding folders	Select one of the following options: • **Scan in real time**: Multimedia Console scans background transcoding folders for new files and adds the files as background transcoding tasks as soon as they are detected. • **Scan 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  .
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**.

17. 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.

18. Notification Center

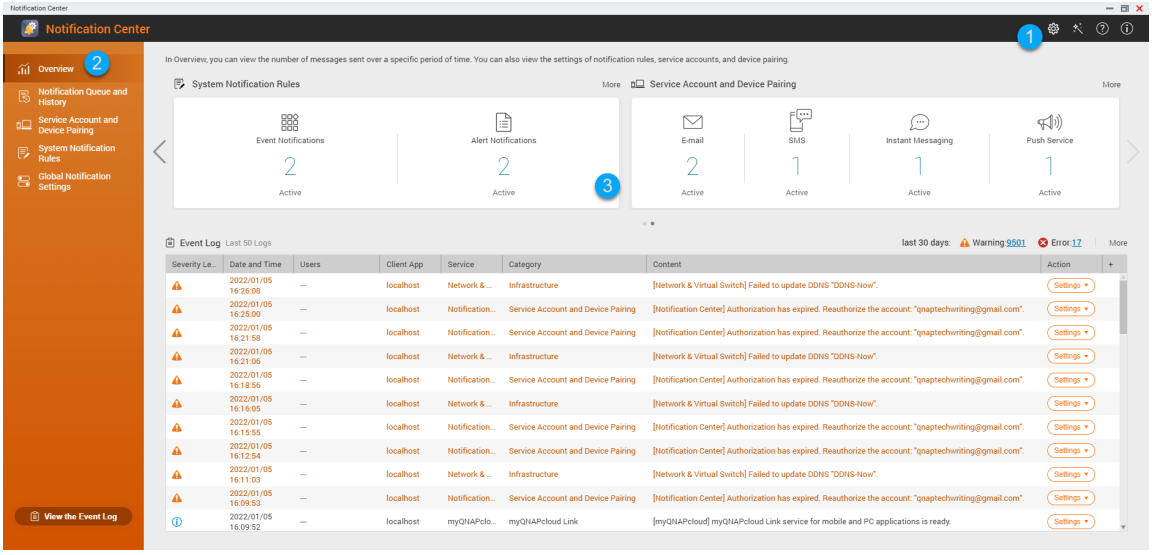
About Notification Center

Notification Center consolidates all QuTS hero 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, 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 devices with your NAS to receive notifications through 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
Gmail or Outlook	a. Click **Add account**. The email account window appears. b. Specify the email address that will act as the sender for QuTS hero notifications. A confirmation message appears. c. Click **Allow**.

Service Providers	User Actions
Yahoo	**Important** You must configure settings in Yahoo Mail before specifying your account information in Notification Center. **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 QuTS hero 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.

Configuring an email server account using Browser Station

You can add an email server account using **Browser Station** authentication to secure your remote email server without setting up a VPN.

Important
Before using **Browser Station** to authenticate an email server account, ensure that:

- You have **File Station** access permission.
- **Container Station** is installed on your device.
- Any proxy server you are using to access **Browser Station** supports WebSocket.
- For details, see:
  - How to Use Browser Station
  - How to Use Container Station

1. Go to **Service Account and Device Pairing** > **E-mail**.
2. Click **Add SMTP Service**.
   The **Add SMTP Service** window appears.
3. Click **Authenticate with Browser Station**.
   The **Browser Station** window appears.

   Note
   It may take a few minutes for the **Browser Station** window to load.

4. Specify your gmail account.
5. Click **Next**.
6. Enter your password.
7. Click **Next**.
   A warning appears.

8. Click **Allow**.
   Add SMTP Service window appears.
9. Optional: Select **Set as default SMTP service account**.
10. Click **Create**.
    The SMTP service is added.

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.

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

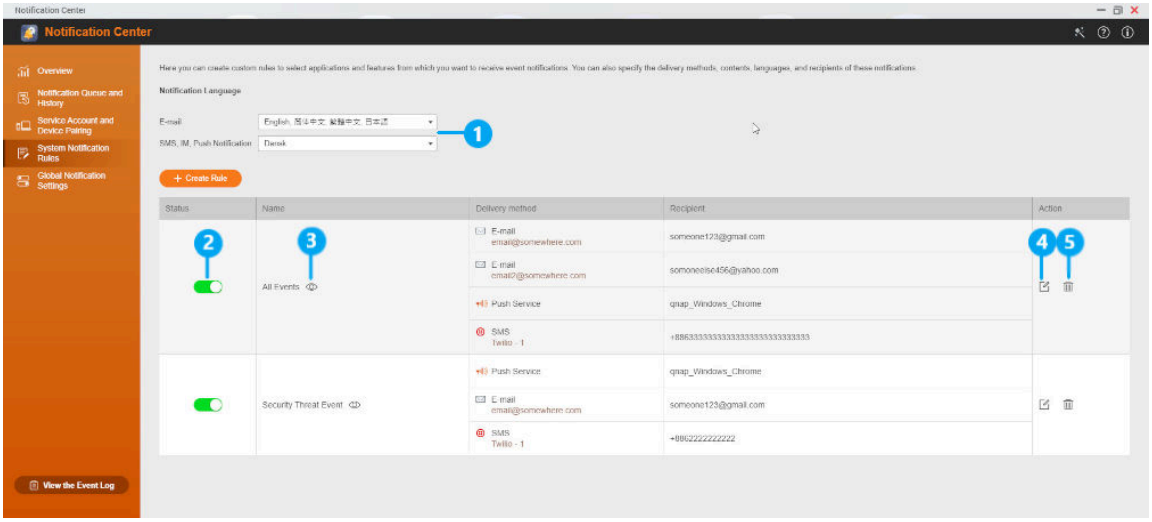
You can create and manage event notification rules in the **Event Notifications** page to receive event notifications promptly.

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, 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 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. 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 event notification filter only accepts keywords that are in English or in any of the languages specified on the **Event Notifications** screen.

8. Optional: 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**. **d.** Optional: Add an email account using **Browser Station**. For details, see Configuring an email server account using Browser Station.
SMS	Select an SMSC server. **Note** To add an SMSC server, see Configuring an SMS Notification Server.
Push Service	Notification Center automatically assigns QBot.

12. Configure the recipient information.

Method	User Action
Email	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **Tip** • To add a recipient, click **Add**, and then specify their email address. • To delete a recipient, click  .
SMS	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then specify their cell phone number. • To delete a recipient, click  .
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.
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  .

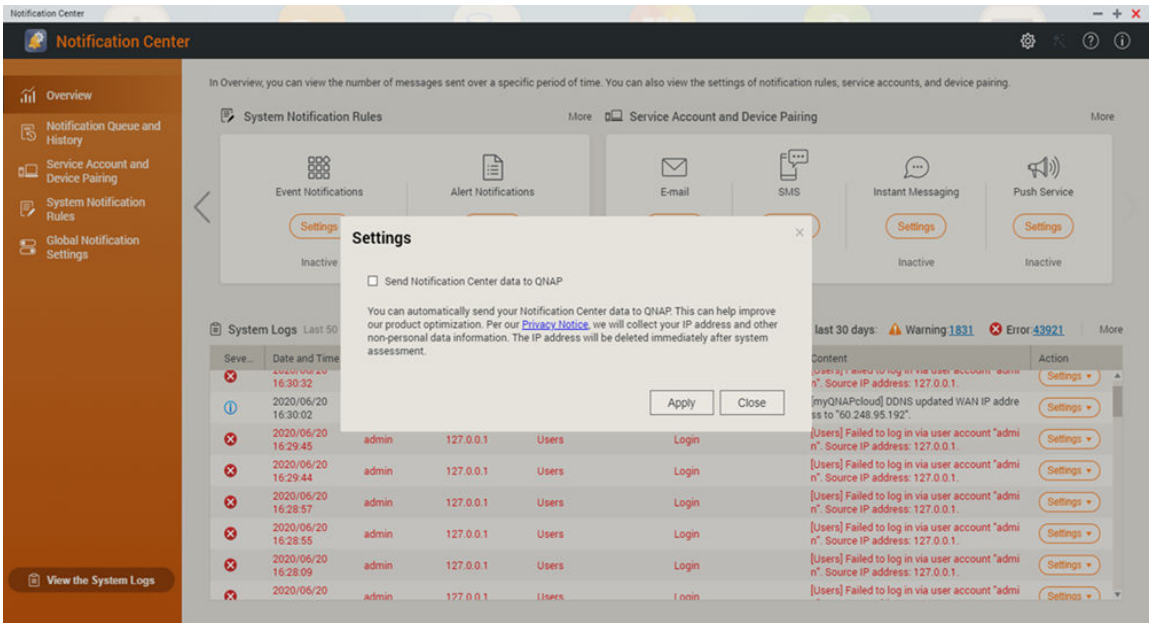
Method	User Action
SMS	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then specify their cell phone number. • To delete a recipient, click  .
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.

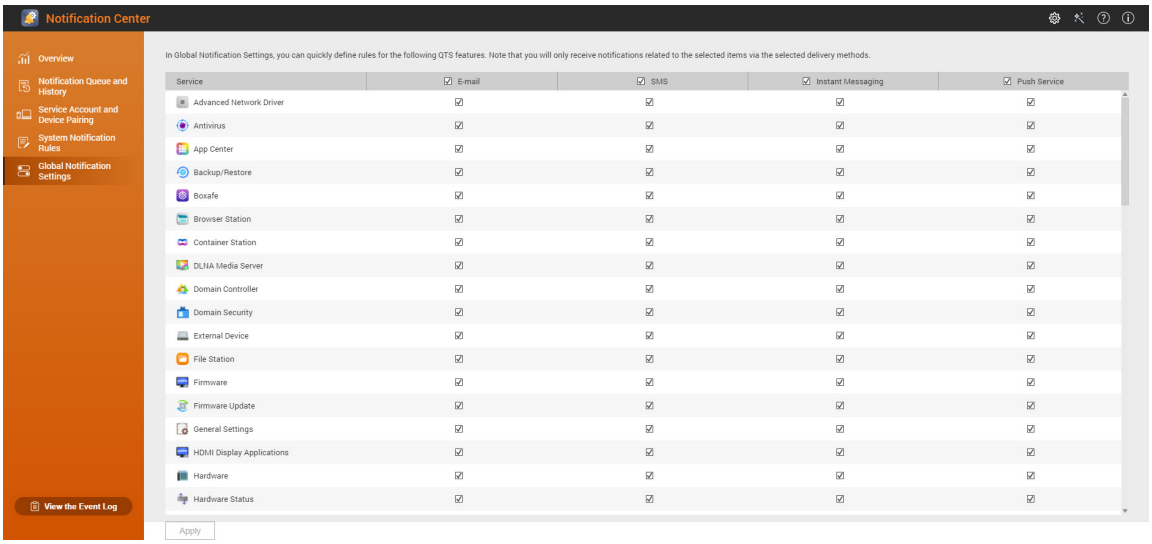
1. Open **Notification Center**.
2. Click .
   The **Send Notification data to QNAP** window appears.
3. Deselect **Send Notification data to QNAP**.
4. Click **Apply**.

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 QuTS hero feature or application.

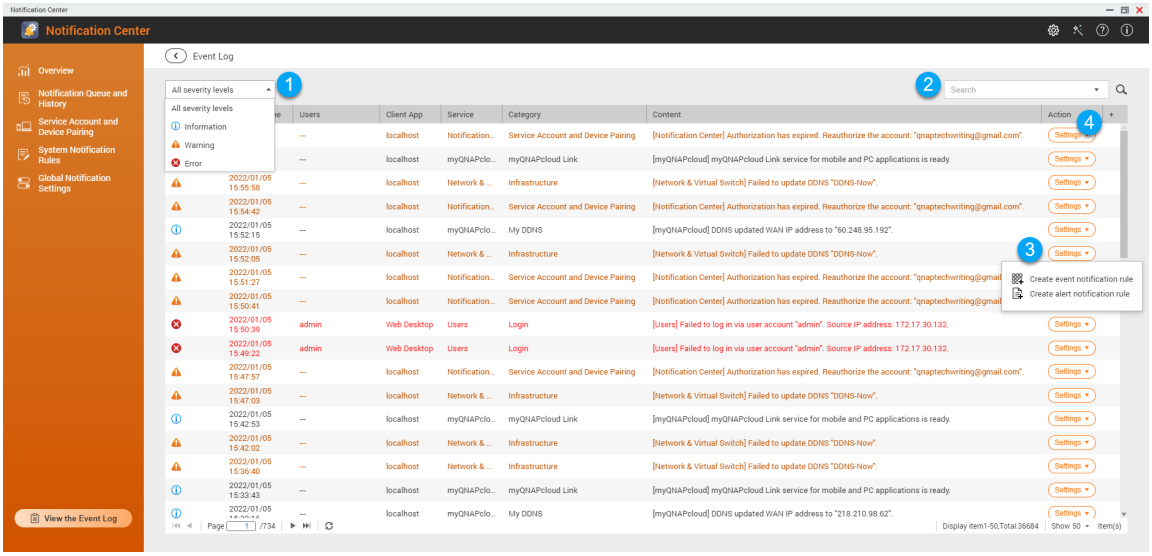
Users only receive notifications related to the selected features through their selected delivery methods.

> **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.

19. 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.

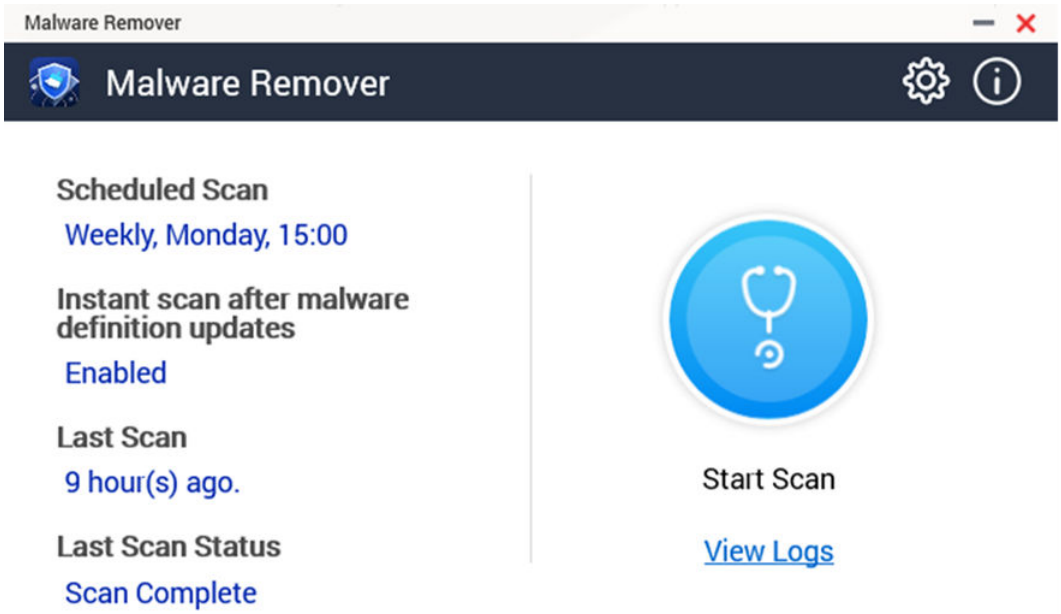
Implementing several layers of protection, Malware Remover allows you to perform instant and scheduled scans on your QNAP device and prevents malicious software from putting your data at risk.

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.

Enabling Ransomware Guard

Ransomware Guard provides continuous protection by monitoring the system for suspicious encryption behavior and isolating files that may pose a threat. When you enable this feature, the application actively scans for ransomware-like activity, automatically blocking and quarantining any files or executables that behave abnormally. This helps prevent unauthorized data encryption and minimizes the impact of potential ransomware attacks.

1. Open Malware Remover.

2. Click **Ransomware Guard**.
3. Click .

Malware Remover enables **Ransomware Guard** on the device.

Note

- To enable Ransomware Guard, click . When prompted, enter your device account password and click **Verify**.
- To view details of the quarantined item, click under **Details** in the **Ransomware Guard** page.

Managing quarantined items

Quarantine Management allows you to review and control files that were automatically isolated by Ransomware Guard. In this page, you can view details about each quarantined item and determine whether it is safe to restore or should be permanently deleted. If you choose to release a file, it is returned to the system but continues to be monitored for abnormal behavior and may be quarantined again if necessary.

1. Open Malware Remover.
2. Click **Ransomware Guard**.
3. Click **Quarantine Management**.
4. Perform any of the following tasks.

Task	User Action
Delete a quarantined item	**a.** Click **Quarantined Programs**. **b.** Identify a quarantined item. **c.** Under **Actions**, click . The **Delete Program** window appears. **d.** Optional: Enter a note explaining the reason for deleting the quarantined file. **e.** Enable **I agree to delete this file**. **f.** Click **Delete**.

Task	User Action
Release a quarantined item	**a.** Click **Quarantined Programs**. **b.** Identify a quarantined item. **c.** Under **Actions**, click  . The **Release Program** window appears. **d.** Optional: Enter a note explaining the reason for releasing the quarantined file. **e.** Enable **I agree to release this file**. **f.** Click **Release**.
Quarantine a released item	**a.** Click **Released Programs**. **b.** Identify a released item. **c.** Under **Actions**, click  . The **Quarantine Program** window appears. **d.** Optional: Enter a note explaining the reason for quarantining the released file. **e.** Enable **I agree to quarantine this file**. **f.** Click **Quarantine**.
View operational logs	**a.** Click **Operational Logs**. **b.** Identify an item. **c.** Review the history of detections, quarantines, and file actions performed by Ransomware Guard.

20. 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 QuTS hero 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 **Yes**.
   The **Enable Remote Support** window appears.
8. 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.

21. 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 QuTS hero User Guide. Currently, disabling Console Management only applies to QuTS hero.

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.