QuTS hero 4.5.x

User Guide

Document Version: 7
28/09/2021

Contents

1. Overview

About QuTS hero....10
What's New in QuTS hero....11
Support and Other Resources....14
NAS Access....15
- Accessing the NAS Using a Browser....16
- Accessing the NAS Using Qfinder Pro....16
- Accessing the NAS Using Qmanager....17
- 2-step Verification....17

QuTS hero Navigation....19
- Task Bar....19
- Main Menu....27
- Desktop....29

Getting Started....33

2. System Settings

General Settings....35
- Configuring System Administration Settings....35
- Configuring Time Settings....37
- Configuring Daylight Saving Time....38
- Configuring Codepage Settings....38
- Configuring Region Settings....39
- Configuring the Login Screen....39
- Configuring Console Management....39

Security....39
- Configuring the Allow/Deny List....40
- Configuring IP Access Protection....40
- Configuring Account Access Protection....41
- SSL Certificate & Private Key....41
- Configuring the Password Policy....43

Hardware....44
- Configuring General Hardware Settings....44
- Configuring Audio Alert Settings....45
- Configuring the Backup Battery Unit (BBU) Settings....45
- Configuring Smart Fan Settings....45
- Configuring Hardware Resource Settings....46
- Viewing SR-IOV Device Settings....47

Power....48
- EuP Mode....48
- Wake-on-LAN (WOL)....48
- Power Recovery....48
- Power Schedule....49

Firmware Update....49
- Firmware Update Requirements....50
- Checking for Live Updates....50
- Updating the Firmware Automatically....51
- Updating the Firmware Manually....52
- Updating the Firmware Using Qfinder Pro....53

Backup/Restore....54
- Backing Up System Settings....54
- Restoring System Settings....54

System Reset and Restore to Factory Default..... 54
External Device.....56
USB Printer.....56
Uninterruptible Power Supply (UPS).....57
System Status.....59
Resource Monitor..... 60

3. Privilege Settings

Users.....61
Default Administrator Account.....61
Creating a Local User.....63
Creating Multiple Users.....65
User Account Lists.....66
Importing Users..... 67
Exporting Users.....68
Modifying User Account Information.....69
Deleting Users..... 71
Home Folders..... 71
User Groups.....72
Default User Groups..... 72
Creating a User Group.....72
Modifying User Group Information..... 73
Deleting User Groups..... 74
Shared Folders..... 74
Default Shared Folders..... 74
Creating a Shared Folder.....75
Editing Shared Folder Properties..... 78
Refreshing a Shared Folder.....80
Removing Shared Folders..... 80
ISO Shared Folders.....80
Shared Folder Permissions..... 82
Folder Aggregation.....86
Shared Folder Encryption.....89
Shared Folder Access.....90
Quota.....95
Enabling Quotas.....96
Editing Quota Settings.....96
Exporting Quota Settings.....97
Quota Conflicts.....97
Domain Security.....97
Active Directory (AD) Authentication..... 98
Azure Active Directory Single Sign-On (SSO)..... 100
LDAP Authentication.....102
AD and LDAP Management..... 103
Domain Controller.....105
Enabling a Domain Controller.....105
Resetting a Domain Controller.....106
Default Domain User Accounts.....106
Creating a Domain User.....107
Creating Multiple Domain Users.....108
Domain User Account Lists.....108
Modifying Domain User Account Information.....110
Deleting Domain Users..... 111
Domain User Groups.....112
Computers.....113
DNS.....115
Back Up/Restore.....118

4. Services

Antivirus....119
Enabling Antivirus....119
Scanning Shared Folders....119
Managing Scan Jobs....121
Managing Reported Scan Jobs....121
Managing Quarantine Files....122
Servers....122
Web Server....122
Enabling LDAP Server....126
SQL Server....127
Syslog Server....128
RADIUS Server....130
Enabling TFTP Server....132
Enabling NTP Server....133

5. File Station

Overview....134
About File Station....134
System Requirements....134
Supported File Formats....134
Parts of the User Interface....135
Settings....137
File Operations....140
Uploading a File....141
Downloading a File....142
Opening a File....142
Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension....143
Opening a Text File Using Text Editor....143
Viewing a File in Google Docs....144
Viewing a File in Microsoft Office Online....144
Opening Image Files Using Image2PDF....145
Viewing File Properties....145
Modifying File Permissions....146
Sorting Files....147
Copying a File....147
Moving a File....148
Renaming a File....149
Deleting a File....150
Restoring a Deleted File....150
Mounting an ISO File....151
Unmounting an ISO File....151
Compressing a File....151
Sharing a File or Folder by Email....152
Sharing a File or Folder on a Social Network....155
Sharing a File or Folder Using Share Links....156
Sharing a File or Folder with a NAS User....158
Playing an Audio File....160
Playing a Video File....160
Playing a Video File Using CAYIN MediaSign Player....161
Opening a 360-degree Image or Video File....161
Streaming to a Network Media Player....162
Adding a File to the Transcoding Folder....162
Canceling or Deleting Transcoding....163
Viewing Transcode Information....164

Extracting Compressed Files or Folders....164
Folder Operations....165
Uploading a Folder....165
Uploading a Folder Using Drag and Drop....166
Viewing Folder Properties....166
Viewing Storage Information....167
Modifying Folder Permissions....168
Viewing Qsync Folders....169
Managing Share Links....169
Viewing Files and Folders Shared with Me....170
Creating a Folder....170
Copying a Folder....170
Creating a Desktop Shortcut....171
Adding a Folder to Favorites....171
Removing a Folder from Favorites....172
Compressing a Folder....172
Deleting a Folder....173
Creating a Shared Folder....174
Sharing Space with a New User....177
Adding a Folder to the Transcoding Folder....177
Canceling or Deleting Transcoding....178
Locking or Unlocking an Encrypted Shared Folder....179
Keeping a Folder or a File in Reserved Cache....179
Removing a Folder from Reserved Cache....180

6. Storage & Snapshots

QNAP Flexible Storage Architecture....182
Global Settings....183
Storage Global Settings....183
Disk Health Global Settings....183
Snapshot Global Settings....184
Storage....185
Disks....185
Storage Pools....191
Shared Folders....200
RAID....210
Self-Encrypting Drives (SEDs)....215
Expansion Units....218
Expansion Unit Actions....219
Expansion Unit Automatic Recovery....219
QNAP External RAID Devices....219
QNAP JBOD Enclosures....229
Snapshots....231
Snapshot Storage Limitations....231
Snapshot Creation....231
Snapshot Management....233
Snapshot Data Recovery....235
Snapshot Clone....238
Snapshot Replica....239
Cache Acceleration....249
Cache Acceleration Requirements....249
Creating the SSD Cache....249
Configuring SSD Cache Disks....250
Configuring Cached Storage....251
Removing the SSD Cache....251
External Storage....251
External Storage Device Actions....252

External Storage Disk Actions....252
External Storage Partition Actions....252
Formatting an External Storage Partition....252
Remote Disk....254
Remote Disk Limitations....254
Adding a Remote Disk....254
Remote Disk Actions....256
VJBOD (Virtual JBOD)....256
VJBOD Requirements....256
VJBOD Limitations....257
VJBOD Automatic Reconnection....257
VJBOD Creation....257
VJBOD Management....261
VJBOD Cloud....264
Installation....264
VJBOD Cloud Volume and LUN Creation....265
Overview....277
Transfer Resources....280
Event Logs....282
Licenses....282
SnapSync....284
SnapSync Requirements....284
SnapSync Restrictions....285
SnapSync Job Creation....285
SnapSync Screen....289

7. iSCSI & Fibre Channel

Storage Limits....293
iSCSI Storage Limits....293
Fibre Channel Storage Limits....293
iSCSI & Fibre Channel Global Settings....293
Creating a Block-Based LUN....293
iSCSI....295
Getting Started with iSCSI....295
iSCSI Performance Optimization....296
iSCSI Storage....296
Fibre Channel....305
FC Ports....305
FC Storage....308
FC WWPN Aliases....309
LUN Import/Export....312
Creating a LUN Export Job....312
Importing a LUN from an Image File....313
LUN Import/Export Job Actions....314
LUN Import/Export Job Status....314

8. ZFS Pool Profiling Tool

Storage Pool Over-Provisioning....316
Creating a Storage Pool Over-Provisioning Test....316
Test Reports....317
Settings....318

9. Network & Virtual Switch

About Network & Virtual Switch....319
Basic and Advanced Mode....319
Overview....319

Interfaces....319
IP Address....320
DNS....322
Virtual LANs (VLANs)....323
Port Trunking....324
System Default Gateway....325
USB QuickAccess....326
Wi-Fi....327
Thunderbolt....337
Virtual Switches....339
Creating a Virtual Switch in Basic Mode....340
Creating a Virtual Switch in Advanced Mode....340
Creating a Virtual Switch in Software-defined Switch Mode....343
DHCP Server....344
Creating a DHCP Server....344
DHCP Clients....347
RADVD....347
Route....350
Creating a Static Route....351
DDNS....351
Adding a DDNS Service....352

10. Network & File Services

About Network & File Services....353
QNAP Service Ports....353
Configuring Network Access Settings....354
Configuring Service Binding Settings....355
Configuring Proxy Server Settings....355
Configuring Network Protocol Settings....356
Configuring Telnet Connections....356
Configuring SSH Connections....356
Editing SSH Access Permissions....357
Configuring SNMP Settings....357
Downloading the SNMP MIB....358
Configuring File Sharing Protocol Settings....359
Configuring Samba (Microsoft Networking) Settings....359
Configuring AFP (Apple Networking) Settings....361
Configuring NFS Service Settings....362
Configuring FTP Settings....363
Configuring Advanced FTP Settings....364
Enabling Service Discovery Settings....364
Enabling the UPnP Discovery Service....365
Enabling the Bonjour Discovery Service....365
Network Recycle Bin Management....365
Configuring the Network Recycle Bin....365
Deleting All Files in the Network Recycle Bin....366
Restricting Access to the Network Recycle Bin....366

11. myQNAPcloud

Getting Started....367
Account Setup....367
Creating a QNAP ID With Email or Phone Number....367
Registering a Device to myQNAPcloud....368
Installing myQNAPcloud Link....369
Overview....369
Configuring UPnP Port Forwarding....370

Configuring DDNS Settings....371
Restarting DDNS Service....371
Configuring Published Services....372
Enabling myQNAPcloud Link....372
Configuring Device Access Controls....372
Installing an SSL Certificate....373

12. App Center

Navigation....375
Left Panel....375
Toolbar....375
Main Area....376
App Management....377
Viewing App Information....377
Installing an App from App Center....378
Installing an App Manually....378
Updating an App....379
Batch Updating Multiple Apps....379
Enabling or Disabling an App....380
Migrating an App....380
Granting or Denying User Access to an App....380
Uninstalling an App....381
App Center Settings....381
Adding an App Repository....381
Configuring App Update Settings....382
Digital Signatures....382
Enabling Installation of Apps without Digital Signatures....382

13. Licenses

About QNAP Licenses....384
License Types and Plans....384
Validity Period....384
License Portals and Utility....385
Software Store....385
License Center....385
License Manager....385
Buying a License Using QNAP ID....386
License Activation....387
Activating a License Using QNAP ID....387
Activating a License Using a License Key....389
Activating a License Using a Product Key or PAK....390
Activating a License Offline....391
License Deactivation....392
Deactivating a License Using QNAP ID....392
Deactivating a License Offline....393
License Extension....394
Extending a License Using QNAP ID....394
Extending a License Offline Using an Unused License....395
Extending a License Offline Using a Product Key....396
Upgrading a License....398
Viewing License Information....399
Recovering Licenses....400
Transferring a License to the New QNAP License Server....400
Deleting a License....401

14. Multimedia

HybridDesk Station (HD Station)....402
Installing HD Station....403
Configuring HD Station....403
HD Station Applications....404
Using HD Player in HD Station....404
DLNA Media Server....405
Enabling DLNA Media Server....405
Configuring DLNA Media Server....405
Media Streaming Add-on....406
Configuring General Settings....406
Configuring Browsing Settings....407
Configuring Media Receivers....408
Multimedia Console....408
Overview....408
Content Management....409
Indexing....410
Thumbnail Generation....411
Transcoding....413
Multimedia App Suite....418

15. QuLog Center

Monitoring System Logs....422
System Event Log....422
System Access Logs....422
Local Logs....423
Local System Event Logs....423
Local System Access Logs....426
Viewing Online Users....428
Creating a Custom Filter Tab for Local Device System Logs....429
Local Log Settings....432
QuLog Service....436
Configuring Log Sender Settings....436
Configuring Log Reciever Settings....438
Viewing and Managing Remote Logs....441
Notification Settings....449
Configuring Notification Rule Settings....449
Adding a Log Filter....450
Editing a Log Filter....451
Removing a Log Filter....451

16. Notification Center

Overview....453
Notification Queue and History....453
Queue....453
History....453
Service Account and Device Pairing....454
Email Notifications....455
SMS Notifications....457
Instant Messaging Notifications....459
Push Notifications....461
System Notification Rules....463
Managing Event Notification Rules....463
Settings....469
Enabling Send Notification Data to QNAP....470
Disabling Send Notification Data to QNAP....470
Global Notification Settings....471

System Logs....471

17. Malware Remover

About Malware Remover....473
Overview....473
Running a Malware Scan....473
Running a Scheduled Scan....474
Settings....474
Configuring Malware Remover....474

18. Helpdesk

Overview....476
Configuring Settings....476
Help Request....476
Submitting a Ticket....477
Remote Support....478
Enabling Remote Support....478
Extending Remote Support....478
Disabling Remote Support....478
Diagnostic Tool....479
Downloading Logs....479
Performing an HDD Standby Test....479
Performing an HDD Stress Test....479

19. Console Management

Enabling Secure Shell (SSH)....480
Enabling SSH on the NAS....480
Enabling SSH on the NAS Using Qfinder Pro....480
Accessing Console Management....480
Accessing Console Management from Windows....480
Accessing Console Management from Mac....481
Logging In to Console Management....481
Managing Existing Applications....481
Activating or Deactivating a License....482
Sorting and Filtering System Logs....483
Showing Network Settings....485
Restoring or Reinitializing the Device....485
Rebooting the NAS....485
Rebooting the Device Into Rescue Mode....485
Rebooting the Device Into Maintenance Mode....486

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

Version	New Features
QuTS hero h4.5.4	We have added the following new features and enhancements for this release to further ensure data and device security. • App Center now checks for available updates every day and automatically installs required updates by default. • QuTS hero now automatically disables applications that are not updated and that do not meet the minimum version requirements. • QuTS hero now displays a message to remind users to disable the default "admin" account and to create another administrator account. • QuTS hero now enables the default "admin" account and resets its password when users press the Reset button on the NAS for three seconds. Nevertheless, to ensure device security, we recommend disabling the "admin" account and using a new administrator account after you finish resetting the system. • UPnP Discovery Service is now disabled by default. • Users can now manually specify the time interval and the maximum number of failed login attempts in Control Panel. • QuTS hero now displays a message to remind users to enable 2-step verification. • Storage & Snapshots now always reserves one snapshot from each time interval when Smart Snapshot Space Management and Smart Versioning are both enabled even when available space is less than 32 GB. • Users can now import custom root certificates to certify the SSL certificate of a server that the NAS needs to access. • Modified the network connection behaviors of containers. • Added support for Content Security Policy HTTP header. • Added an encryption option for SnapSync jobs. Other new features and enhancements: • Added support for enabling SSD over-provisioning on external devices. • Optimized access performance for fast clone files to reduce memory usage. • Improved the user interface of Advanced Search in QuLog Center. • Added support for displaying the total connection time of online users. • All users in the administrator group can now use and manage VJBOD. • All users in the administrator group can now use and manage Snapshot Replica. • File Station now supports displaying thumbnail previews for PDF files.

Version	New Features
QuTS hero h4.5.3	• QuTS hero now automatically installs recommended firmware updates by default. Administrators can specify a schedule to check and perform updates. • QuTS hero now displays supported bus types for all slots on the NAS. • QuTS hero now supports Kernel-Mode SMB Daemon. Enabling this feature disables SMB encryption. • QuTS hero now displays SSD status as "warning" when estimated lifespan drops below the threshold. • QuTS hero now supports sharing up to 100,000 files or folders via shared links. • App Center now checks for available updates every day and automatically installs required updates by default. • Users can now configure over-provisioning settings based on the test results of ZFS Pool Profiling Tool. • Users can now specify a community name when using UPS with SNMP connection. • Users in the administrator group can now manage all shared links. • To enhance device security, QuTS hero now automatically checks the SQL Server password and disables the service if users still use the default password. Web Server service is now disabled by default. • Modified various HTTP header default configurations to enhance device security.
QuTS hero h4.5.2	• Added support for SnapSync, which allows users to back up their NAS data to another QNAP NAS. • Added support for QNAP SSD Antiwear Leveling (QSAL), which prevents simultaneous SSD failure for better data protection and system reliability. • Added support for SR-IOV. • Users can now create a guaranteed snapshot space dedicated to each shared folder or LUN. • Users can now change thin provisioning to thick provisioning for a shared folder. • Users can now choose to optimize storage performance when creating a storage pool. • Storage & Snapshots now supports displaying the supported bus types of SSD slots.

Version	New Features
QuTS hero h4.5.1	• QuTS hero now provides Console Management, a command-line interface that supports log viewing, app management, license activation, and other operations via SSH. • QuTS hero now supports QuLog Center, which replaces System Logs and allows for centralized log management of system events, system access, and online user status on your devices. • QuTS hero now supports SAS, SATA, and USB JBOD enclosures. • QuTS hero now supports VJBOD Cloud. • Designed for enhancing system security, Malware Remover is now a built-in utility. • File Station now supports HEIC and HEIF images. • File Station now supports playing videos with CAYIN MediaSign Player. • Users can now join the NAS to a domain managed by Azure Active Directory Domain Services. • Modified folder permissions and access right settings for mounted SMB and NFS shared folders.

Version	New Features
QuTS hero h.4.5.0	QuTS hero h4.5.0 is the first public release of the QuTS hero operating system. QuTS hero h4.5.0 offers the following new features: • **ZFS**: An advanced file system, which ensures high performance and data integrity. • **Inline data deduplication**: A block-based data reduction technique performed before data is written to storage. This helps optimize storage usage and reduce storage requirements. • **Inline compression**: Compress data to reduce storage I/O workloads for improved performance. • **Inline compaction**: QuTS hero rearranges how data is stored on SSDs, reducing the amount of space required to store data. This can help deliver higher cost efficiency for all-flash storage systems. • **Data self-healing**: ZFS uses end-to-end checksums to detect and correct silent data corruption caused by hardware defects, bugs in firmware, or metadata errors. • **New RAID types**: QuTS hero adds support for RAID Triple Parity for protecting against three-disk failures, and Triple Mirror for an identical copy of data stored on three disks. • **RAID Z**: Designed to deal with petabytes of data, RAID Z allows you to create ready-to-use high-capacity RAID configurations in a matter of seconds. • **Multi-level cache technology**: QuTS hero supports main memory read cache (L1 ARC), SSD second-level read cache (L2 ARC), and ZFS Intent Log (ZIL) for accelerated read and write performance and improved cache integrity. • **Near limitless snapshots**: Support for up to 65,535 snapshots of iSCSI LUNs and shared folders. If one snapshot is created every hour, 24 snapshots per day, then up to seven years of snapshots can be stored on a single NAS.

For details on new features and enhancements, go to https://www.qnap.com/en/release-notes/.

Support and Other Resources

QNAP provides the following resources:

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

Resource	URL
Community Forum	https://forum.qnap.com
QNAP Accessories Store	https://shop.qnap.com

NAS Access

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

Method	Description	Requirements
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	• Mac computer that is connected to the same network as the NAS • Qfinder Pro

Accessing the NAS Using a Browser

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

> **Tip**
> If you do not know the IP address of the NAS, you can locate it using Qfinder Pro.
> For details, see Accessing the NAS Using Qfinder Pro.

   The 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. Specify your username and password.
6. Click **Login**.
   The QuTS hero desktop appears.

Accessing the NAS Using Qfinder Pro

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

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

2. Open Qfinder Pro.
   Qfinder Pro automatically searches for all QNAP NAS devices on the network.
3. Locate the NAS in the list, and then double-click the name or IP address.
   The 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.

2-step Verification

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

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

Enabling 2-step Verification

1. Install an authenticator application on your mobile device.
   QuTS hero supports the following applications:

- Google Authenticator: Android, iOS, and BlackBerry
- Authenticator: Windows Phone

2. Verify that the system times of the NAS and mobile device are synchronized.

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

3. In QuTS hero, go to **Options** > **2-step Verification** .
4. Click **Get Started**.
The **2-step Verification** window opens.
5. Open the authenticator application on your mobile phone.
6. Configure the application by scanning the QR code or specifying the security key displayed in the **2-step Verification** window.
7. In the **2-step Verification** window, click **Next**.
The **Confirm your 2-step verification settings** screen appears.
8. Specify the security code generated by the authenticator application.
9. Select an alternative verification method that will be used whenever your mobile device is inaccessible.

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

10. Click **Finish**.

Logging in to QuTS hero Using 2-step Verification

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

Disabling 2-step Verification

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

QuTS hero Navigation

Task Bar

No.	Element	Possible User Actions
1	**Show Desktop**	Click the button to minimize or restore all open windows.
2	**Main Menu**	Click the button to open the **Main Menu** panel on the left side of the desktop.
3	**Search**	• Type key words to locate settings, applications, and help content. • Click an entry in the search results to open the application, system utility, or **Help Center** window. **Tip** App or utility search results are classified into **Systems**, **Application**, and **Help**.

No.	Element	Possible User Actions

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 the mouse pointer over the button to see the number of background tasks that are running. 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 the mouse pointer over the button to view the number of external storage devices and printers that are connected to the USB and SATA ports on the NAS. • Click the button to view the details for each connected device. • Click a listed device to open File Station and view the contents of the device.

7	**Event Notifications**	• Hover the mouse pointer over the button to see the number of recent errors, warnings, and notices.
		• Click the button to view the following details for each event:
		  • Event type
		  • Description
		  • Timestamp
		  • Number of instances
		• Click a list entry to view the related utility or application screen. Clicking a warning or error log entry opens the **System Event Log** window.
		• Click **More>>** to open the **System Event Log** window.
		• Click **Clear All** to delete all list entries.

8	**Options**	Click your profile picture to open the **Options** screen.

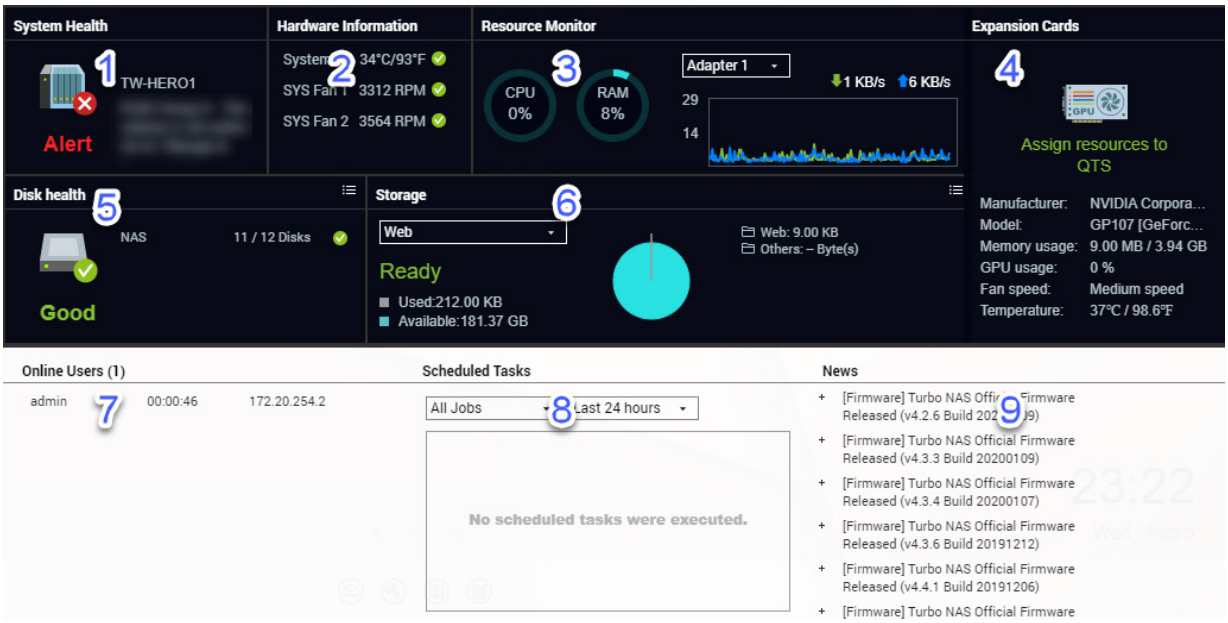
No.	Element	Possible User Actions
9	**[USER_NAME]**	Click the button to view the last login time and the following menu items: • **Options**: Opens the **Options** window • **Sleep**: Keeps the NAS powered on but significantly reduces power consumption **Note** This feature is only available on models 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:
		• **What's New**: Opens the **What's New** window, which displays information on the new features and enhancements available in the installed QuTS hero version
		• **Help**: Displays links to the Quick Start Guide, Virtualization Guide, Help Center, and online tutorials page
		• **Language**: Opens a list of supported languages and allows you to change the language of the operating system
		• **Desktop Preferences**: Opens a list of display modes and allows you to select the mode based on your device type
		• **Help Request**: Opens the Helpdesk window
		• **Data & Privacy**: Opens the **QNAP Privacy Policy** page
		• **About**: Displays the following information:
		  • Operating system
		  • Hardware model
		  • Operating system version
		  • Number of installed drives
		  • Number of empty drive bays
		  • System pool name
		  • Used disk space
		  • Available disk space

11	**Dashboard**	Click the button to display the dashboard.

Dashboard



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

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

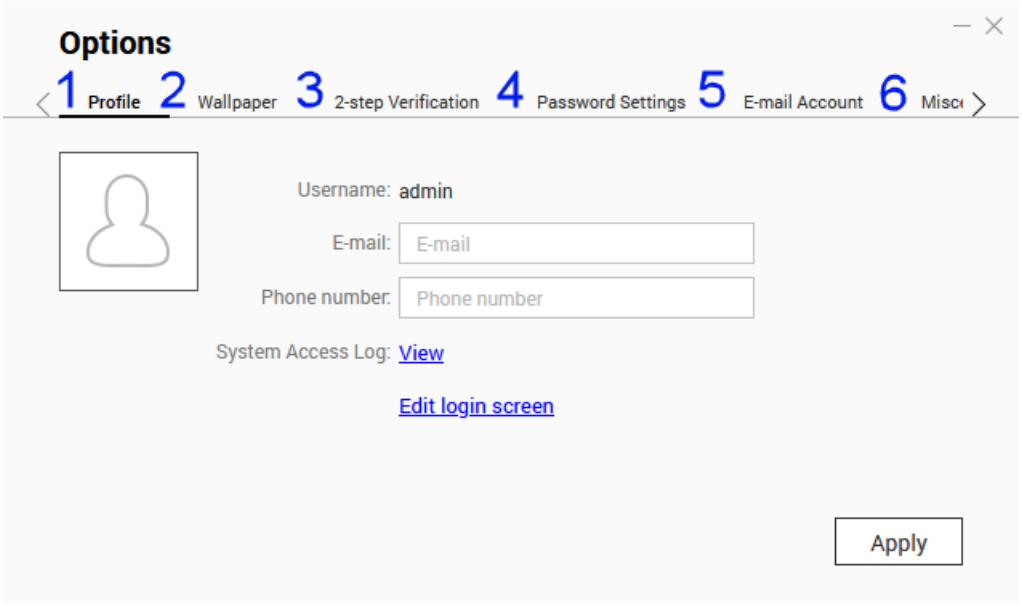
No.	Section	Displayed Information	User Actions
1	System Health	• NAS name • Uptime (number of days, hours, minutes and seconds) • Health status	Click the heading to open **Control Panel** > **System** > **System Status** > **System Information** . If disk-related issues occur, click the heading to open **Storage & Snapshots**.
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 & Snapshots**.
			• Click to switch between disk and NAS information.
			• Click a disk name to view the following information for each installed disk:
			  • Capacity/size
			  • Temperature
			  • Health status
			• Click **Details** to open **Storage & Snapshots** > **Overview** > **Storage** .

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	• Username • IP address • Total connection time • Connection type	Click the heading to open **Control Panel** > **System** > **QuLog Center** > **Online Users** .
8	Scheduled Tasks	• Task type • Task summary • Task name • Timestamp • Status	Use the filters to view tasks that were executed within a specific period.
9	News	Links to QNAP announcements	Click the heading to open the relevant pages on the QNAP website.

Options



#	Tab	Possible User Actions

1	**Profile**	• Specify the following optional information:
		  • Profile picture
		  • E-mail
		  • Phone number
		• Click **View** to open the **System Connection Logs** screen.
		• Click **Edit login screen** to open the **Login Screen** configuration screen in the **Control Panel** window.
		• Click **Apply** to save all changes.

2	**Wallpaper**	• Select a wallpaper from the built-in options or upload a photo. • Click **Apply** to save all changes.
3	**2-step Verification**	Click **Get Started** to open the configuration wizard.

4	**Change Password**	• Specify the following information:
		  • **Old password**
		  • **New password**: Specify a password with a maximum of 64 characters. QNAP recommends using passwords with at least 6 characters.
		• Click **Apply** to save all changes.

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

#	Tab	Possible User Actions

6	**Miscellaneous**	• Enable the following settings.
		  • **Auto logout after an idle period of**: You can 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.
		  • **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

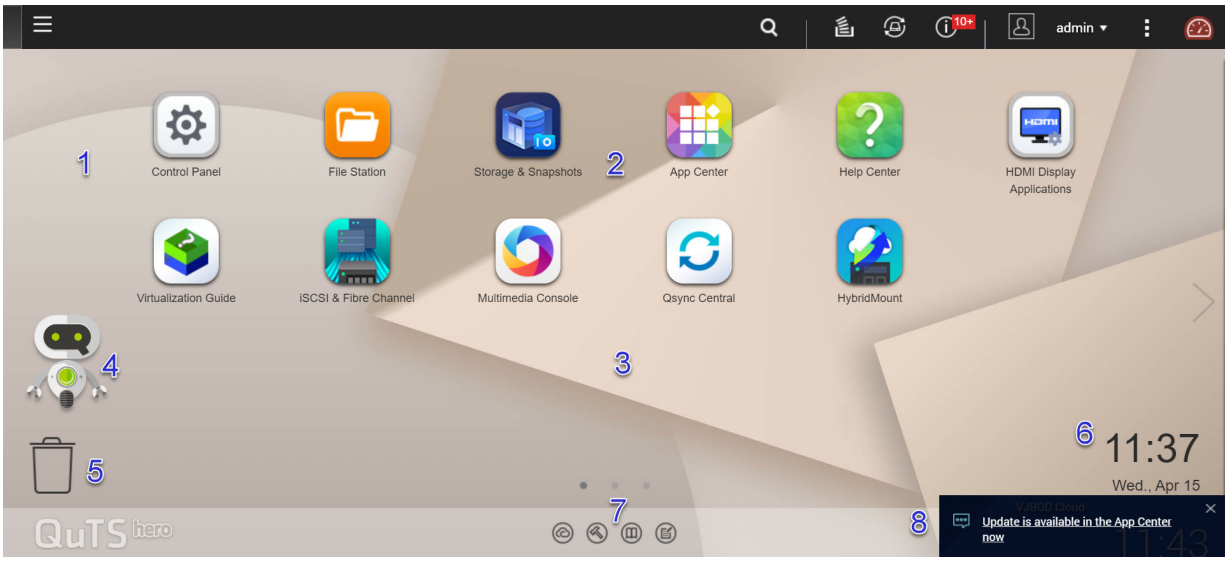
No.	Section	Description	Possible User Actions
1	NAS Information	Displays the NAS name and model number.	N/A

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 & Snapshots
		• iSCSI & Fibre Channel
		• Users
		• Network & Virtual Switch
		• myQNAPcloud
		• Resource Monitor
		• App Center
		• Help Center
		• Qboost
		• HDMI Display Applications
		Note
		This menu item only appears on models with certain hardware specifications.
			• Open a system utility or application in the 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.

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	

Desktop



#	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.

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 & Snapshots
		• App Center
		• Help Center
			• Click an icon to open the application window.
			• Right-click an icon and then select one of the following:
			  • **Open**: Opens the application window
			  • **Remove**: Deletes the icon from the desktop
			• Click and drag an icon to another desktop.

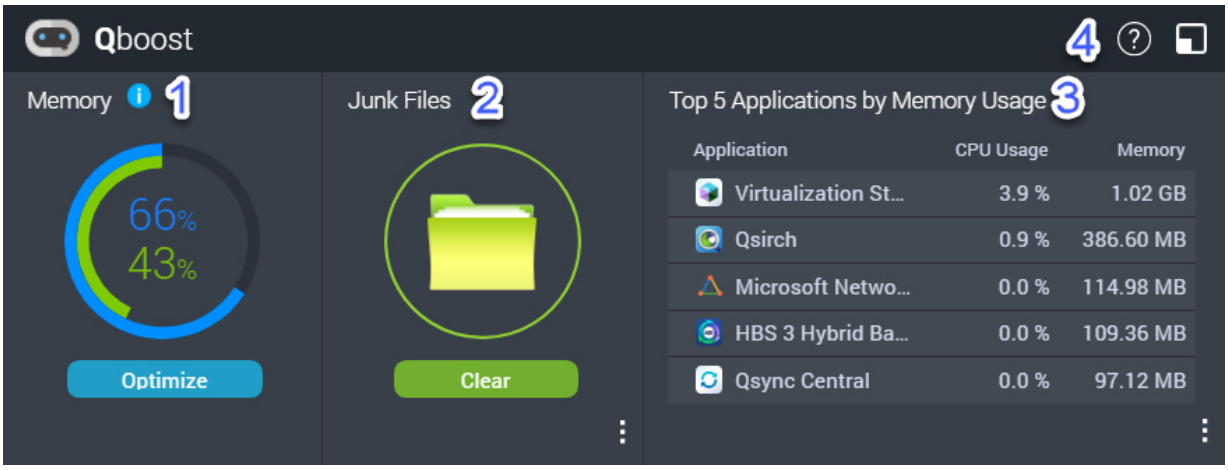
3	Desktop	This area contains open system utilities and applications. The desktop consists of three separate screens.	Click **<** or **>** to move to another desktop.
4	Qboost	This enables you to manage and monitor memory consumption.	• Click or to display the memory status and open the Qboost panel. • Click or to hide the memory status and close the Qboost panel.

#	Element	Description	Possible User Actions

5	Recycle Bin	This displays the list of files that the currently active user moved to the Recycle Bin.
		The following applications provide users a choice between permanently deleting files and moving files to the Recycle Bin.
		• File Station
		• Music Station
		• Photo Station
		• Video Station
			• Click to open the **Recycle Bin** screen in the **File Station** window.
			• Right-click and then select one of the following:
			  • **Open**: Opens the **Recycle Bin** screen in the **File Station** window
			  • **Empty All**: Permanently deletes files in the Recycle Bin
			  • **Settings**: Opens the **Network Recycle Bin** screen in the **Control Panel** window

6	Date and time	This displays the date and time that the user configured during system installation.	N/A
7	Link bar	This displays shortcut links to myQNAPcloud, utility and app download pages, feedback channels, and the Helpdesk.	Click any of the following buttons: • : Opens the myQNAPcloud website in another browser tab • : Opens the download page for mobile applications and utilities • : Provides links to the QNAP Wiki, QNAP Forum, and Customer Service portal • : Opens the Helpdesk utility
8	Notifications	This notifies the user about important system events that may or may not require user action. Notifications appear in the lower right corner of the desktop.	Click the notification to open the corresponding utility or app.

Qboost



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

#	Section	Description	User Actions
1	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.

#	Section	Description	User Actions
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.

Getting Started

1. Log in to the NAS as an administrator.
   The default administrator account is `admin`.
   For details, see NAS Access.
2. Optional: Create one or more storage pools.
   For details, see Creating a Storage Pool.
3. Create one or more shared folders.
   You must create at least one shared folder in order to store files on the NAS.
   For details, see Creating a Shared Folder.
4. Create user accounts.
   QNAP recommends creating a user account for each person that requires access to the NAS.
   For details, see Creating a Local User.
5. Optional: Create user groups.
   User groups help you to easily manage user accounts.
   For details, see Creating a User Group.
6. Edit shared folder permissions.

Permissions enable you to control who can view and modify files in a shared folder.
For details, see Shared Folder Permissions.

7. Map the shared folders as network drives on your computer.
   For details, see Shared Folder Access.

8. Store and manage files.
   For details, see File Station.

2. 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.

Field	User Action
Server name	Specify a name containing up to 14 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • 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.
System port	Specify the port used to access the web interface. The default port is 8080.

Field	User Action
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.
Enable secure connection (HTTPS)	Select this option to allow HTTPS connections. **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.** Specify a port number. **d.** Select **Force secure connection (HTTPS) only** to require all users to connect to the NAS using only HTTPS.
Custom HTTP server header	Select this option to specify a server HTTP header.
Do not allow QuTS hero embedding in IFrames	**a.** Select this option to prevent websites from embedding QuTS hero using IFrames. **b.** Click **Allowed Websites** to allow a specific website to embed QuTS hero in IFrames. **c.** The **Allowed Websites** window appears. **d.** Click **Add** to add a website to the list. **e.** The **Add Host Name** window appears. **f.** Specify a host name. **g.** Click **Add**. The host name is added to the allowed websites list. **h.** Select a website, and then click **Delete** to delete a website from the list. **i.** Click **Apply**.
Enable X-Content-Type-Options HTTP header	Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities.
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.

Field	User Action
Redirect URL to 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. **Tip** You can check the web server settings by going to **Control Panel** > **Applications** > **Web Server** . Select this option to enable redirecting the URL to the NAS login page.

3. Click **Apply**.

Configuring Time Settings

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

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

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

Option	User Action
Manual setting	Specify the date and time.
Synchronize with a time server automatically	Ensure that your NAS is connected to the Internet, and then specify the following information: • **Server**: Name of the Network Time Protocol (NTP) server Examples: time.nist.gov, time.windows.com • Optional: Click **Test Connection**. The system will test if a connection can be established with the configured time server. • **Time interval**: Number of hours or days between each time synchronization task

Option	User Action
Set the server time the same as your computer time	Click **Update**.

5. Click **Apply**.

Configuring Daylight Saving Time

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

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

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

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

Configuring Codepage Settings

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

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

Configuring Region Settings

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

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

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

3. Click **Apply**.

Configuring the Login Screen

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

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

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

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

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.	**a.** Select **Deny connections from the list**. **b.** Click **Add**. The IP configuration window appears. **c.** Specify an IP address, netmask, or IP range. **d.** Click **Create**. **Tip** To remove an IP address, netmask, or IP range, select an entry from the table, and then click **Remove**.
Use IP allow list	The NAS can only connect to the IP addresses or network domains included in the IP allow list.	**a.** Select **Allow connections from the list only**. **b.** Click **Add**. The IP configuration window appears. **c.** Specify an IP address, netmask, or IP range. **d.** Click **Create**. **Tip** To remove an IP address, netmask, or IP range, select an entry from the table, and then click **Remove**.

3. Click **Apply**.

Configuring IP Access Protection

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.
   - Time period
   - Maximum number of unsuccessful login attempts within the time period
   - Amount of time the IP will be blocked
4. Click **Apply**.

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

Transport Layer Security (TLS) is a protocol used for secure data transfers and encrypted communication between web servers and browsers. You can upload a Secure Sockets Layer (SSL) certificate from a trusted provider through Server Certificate or import a custom root certificate to your QNAP device to certify the SSL certificate of a server. 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.

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

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 and private key. **b.** Optional: Click **Browse** to upload an intermediate certificate.
Get from Let's Encrypt	**a.** Specify a domain name containing a maximum of 63 ASCII characters, without spaces. **b.** 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** > **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. The maximum length of a password is 64 characters.

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

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

   a. Select **Require users to change passwords periodically**.

   b. Specify the maximum number of days that each user password is valid.

   c. Optional: Select **Send a notification email to users a week in advance of their password expiring**.

4. Click **Apply**.

Hardware

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

Configuring General Hardware Settings

1. Go to **Control Panel** > **System** > **Hardware** > **General** .

2. Configure the following settings.

Settings	User Action
Enable configuration reset switch	Select this option to enable the reset button. For details, see System Reset and Restore to Factory Default.
Enable disk standby mode	Select this option to allow the NAS drives to enter standby mode if there is no disk access within the specified period. Disk status LED remains on during standby mode.
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 the redundant power supply.

Settings	User Action
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.

3. Click **Apply**.

Configuring Audio Alert Settings

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

Setting	Description
System operations	Select this option to trigger an audio alert every time the NAS starts, shuts down, or upgrades firmware.
System events	Select this option to trigger an audio alert when errors or warnings occur.

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 TPU modules or network expansion cards that support SR-IOV.

For details, see Viewing SR-IOV Device Settings.

1. Go to **Control Panel** > **System** > **Hardware** > **Hardware Resource** .
   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.

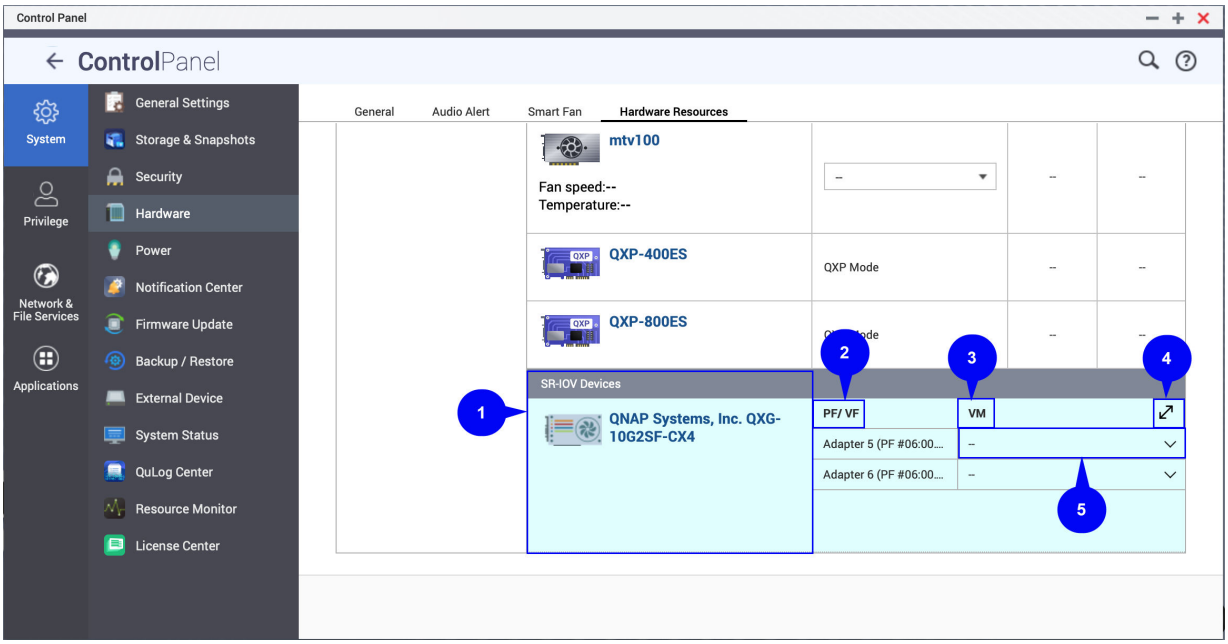
OS or Application	Description
QuTS hero	QuTS hero applications share expansion card resources for transcoding. • Select **Hardware Transcoding** to allow QuTS hero software to use expansion card resources to speed up transcoding tasks. Only one card can be assigned to hardware transcoding. • Select **Output** 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**.

Viewing SR-IOV Device Settings

You can view all Single Root I/O Virtualization (SR-IOV) devices mapped to your virtual machines on the **Hardware Resource** 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.

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.

EuP Mode

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

Configuring EuP Mode

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**.

Wake-on-LAN (WOL)

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

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

Enabling or Disabling Wake-on-LAN (WOL)

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

Power Recovery

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

Configuring the Power Recovery Settings

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

- Keep the NAS turned off.

3. Click **Apply**.

Power Schedule

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

Configuring the Power Schedule

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

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

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 can benefit from new QuTS hero software features, security updates, enhancements, and bug fixes.

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

Update Method	Description
Using **Live Update**	Firmware updates are immediately and automatically detected by QuTS hero. For details, see Checking for Live Updates.
Using **Manual Update**	You can check for latest device firmware updates on the QNAP website, download the firmware update to a computer, and manually install the firmware update onto your device. For details, see Updating the Firmware Manually.

Update Method	Description
Using **Auto Update**	You can configure QuTS hero to periodically check for firmware updates and automatically download and install the specified firmware update version. 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.

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 for updating the firmware manually or through Qfinder Pro. • Ethernet cables **Important** QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection is reliable during firmware updates.
System reboot	QNAP recommends rebooting the NAS system before the firmware backup.
Administrator privileges	You must be a NAS administrator or have admin priveleges to update firmware.
Stop NAS operations	QNAP recommends stopping all other NAS operations before the firmware update. The NAS must be restarted for the firmware update to take effect and 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. • Log on to your device to find the model name.
Firmware version	If you are updating the firmware using **Manual Update** or Qfinder Pro, ensure the selected firmware version is correct for your device model.

Checking for Live 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

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

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

4. Click **Apply**.

Updating the Firmware Automatically

When you enable auto update, it ensures the operating system automatically downloads the most stable and comprehensive version of the firmware. QNAP recommends enabling this feature for optimal firmware stability and security.

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.
- All ongoing tasks will be suspended during the auto update.
- QNAP recommends enabling this feature after testing the Checking for Live Updates feature on your device.

1. Go to **Control Panel** > **System** > **Firmware Update** > **Auto Update** .
2. Specify the auto update time.
3. Select the auto update firmware version.

Note
QNAP recommends selecting the recommended version, which includes bug fixes from multiple releases for firmware auto update.

4. Click **Apply**.
   - You will receive email notifications about available firmware updates.
   - QuTS hero automatically downloads the available stable version firmware during the specified update time.

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** > **Firmware Update** .
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** > **System Event Logs** 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 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 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**.

Backup/Restore

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

Backing Up System Settings

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

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

Restoring System Settings

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

1. Go to **Control Panel** > **System** > **Backup/Restore** > **Backup/Restore Settings** .
2. Click **Browse**.
3. Select a valid BIN file that contains the QuTS hero system settings.
4. Click **Restore**.

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.
- The default "admin" account is automatically enabled after the system reset.

- To protect your device from attacks, QNAP recommends disabling the default "admin" account after a system reset. To disable the account, change the default admin password, log out of QuTS hero, and then log in to QuTS hero with another admin account.

Option	Description	Steps

Basic system reset	This resets the following settings to the default values without deleting the user data stored on the disks.
	• System administrator password: MAC address of adapter 1 without special characters (all letters must be uppercase). For example, if the MAC address of adapter 1 is 11:22:33:AA:BB:CC, then the default admin password will be 112233AABBCC.
	Tip
	You can find the MAC address of adapter 1 using Qfinder Pro. It is also printed on a sticker on the device as "MAC1".
	• 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.

Option	Description	Steps
Advanced system reset	This performs a basic system reset and then restores the QuTS hero default settings, deleting all users, user groups, and shared folders previously created. The user data stored on the disks is retained. **Note** To retrieve old data after an advanced system reset, re-create the previous folder structure on the NAS.	Perform an advanced system reset using one of the following methods. • Using QuTS hero: **a.** Go to **Control Panel** > **System** > **Backup/Restore** > **Restore to Factory Default** . **b.** Click **Reset Settings**. **c.** Choose to restart or shut down the NAS after the system is reset. **d.** Click **OK**. • Using the reset button: **a.** Power on the NAS. **b.** Press and hold the reset button for 10 seconds.
Reinitialize the NAS	This 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**. **3.** Choose to restart or shut down the NAS after the NAS is reinitialized. **4.** Click **OK**.

External Device

USB Printer

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

Configuring USB Printer Settings

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

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

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

Task	Action
View printer information	Click **Printer Info**. This displays the details of the selected printer.
View printer log	Click **Printer Log**. This displays the current and completed print jobs on the selected printer. **Tip** You can stop, resume, or cancel ongoing or pending print jobs. You can also delete completed or pending print jobs. Click **Clear** to clear the history.
Clean up spool space	Click **Clean Up Spool Space**. This deletes the data stored in the printer spool.
Configure printer settings	Click **Settings**. This enables you to configure the following settings: • **Stop printer sharing and clear print spool**: Select this option to disable printing and delete all stored data on the selected printer. • **Bonjour printer support**: Select this option to introduce the printing service to the macOS users on your network.

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

Creating a USB Printer Access List

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

1. Go to **Control Panel** > **System** > **External Device** > **USB Printer** .
   QuTS hero displays the detected USB printers on your network.
2. Click **Enable USB printer**.
3. Specify access rights.
   a. Beside **Access right**, select **Allow printing** or **Deny printing**.
   b. Specify the IP addresses or domain names that you want to allow or deny.

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

4. Click **Apply**.

Uninterruptible Power Supply (UPS)

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

NAS Behavior During a Power Outage

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

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

Configuring the UPS Settings

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

Mode	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
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**.

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, dual-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. • Dual-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.
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.

3. 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 admin account, and disabling the default admin account. A new administrator account can perform the same actions as the default administrator account.

The default admin account must be enabled in two specific scenarios. First, if you want to access the QNAP turbo NAS via Secure Shell (SSH) or Telnet, and second, if you're going to access Console Management.

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.
Username	Specify a username that contains 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: . - _ ~ ! @ # $ % ^ & ( ) { }
Password	Specify a password that contains a maximum of 64 ASCII characters.
Phone number (optional)	Specify a phone number that will receive SMS notifications from 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.

Field	Description
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.
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.
Username	Specify a username that contains 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: . - _ ~ ! @ # $ % ^ & ( ) { }
Password	Specify a password that contains a maximum of 64 ASCII characters.
Verify Password	Enter the password again.

Field	Description
Phone number (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.
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: @ " + = / \ : | * ? < > ; [ ] % `' 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`.
Number of Users	Specify the number of users (1–4095). Example: `5`

Field	Description
Password	Specify a password that contains a maximum of 64 ASCII characters.

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

5. Click **Next**.
   QuTS hero creates the user accounts and adds them to the displayed user list.
6. 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`

Important

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

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

- Specify information for only one user on each line.
  Example:
  ```
  John,s8fk4b,100,Sales
  Jane,9fjwbx,150,Marketing
  Mary,f9xn3ns,390,RD
  ```

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`

Important

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

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

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

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

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.

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

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. **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.** Optional: Disable the account. 1. Select **Disable this account**. 2. Select when to disable the acccount. • **Now**: The account will be disabled after clicking **OK**. • **Expiry date**: The account will be disabled on the specified date. **d.** 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. **e.** Click **OK**.
Edit user group	**a.** Under **Action**, click . The **Edit User Group** window appears. **b.** Select or deselect user groups. **c.** Click **Apply**.

Task	User Action
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 the administrator 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. The administrator 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.
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**.

Task	User Action
Edit user group members	**a.** Under **Action**, click . The **Edit User Group** window appears. **b.** Select or deselect users. **c.** Click **Apply**.
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**.

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
Download	This is the default folder for Download Station. The folder stores content downloaded in QuTS hero. You can assign a different path for downloads in Download Station.
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** .

Folder	Description
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

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 the following information:

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : | * ? < > ; [ ] % ` '.
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters. The information is for your reference and is not used by QuTS hero.
Storage Pool	Specify the storage pool where the shared folder will be created.
Space Allocation	Select one of the following space allocation options: • **Thick provisioning** • **Thin provisioning**
Allocate folder quota	Specify the maximum size of the shared folder.

4. Configure storage settings.

Field	Description
Data reduction	• **Compression** • **Deduplication**
Performance	• **SSD cache** **Note** You must create and enable SSD cache to select this option • **Fast clone**: This option allows you to copy data faster within individual shared folders and LUNs.
Synchronous I/O	• **Auto** • **All** • **None**
Performance profile (block size)	Select the block size for I/O acceleration.

5. Optional: Configure user access permissions.
   a. Under **Configure access privileges for users**, click **Edit**.
   b. Specify the access permissions for users.
   For details, see Shared Folder Permissions.
6. Optional: Enable folder encryption.
   a. Under **Folder Encryption**, click **Edit**.
   b. Select **Encryption**.
   Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.
   c. Specify the following information.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " $: = \ This field does not support multibyte characters.
Verify Password	The password must match the previously specified password.

Field/Option	Description
Save encryption key	When enabled, QuTS hero automatically unlocks the shared folder after the NAS restarts. When disabled, the administrator must unlock the folder after the NAS restarts. For details, see Unlocking a Shared Folder. **Note** QNAP strongly recommends exporting and saving the encryption key. For details, see Configuring Encryption Settings. **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 shared folder will become inaccessible and all data will be lost.

7. Configure WORM settings.

Note

- When Write Once Read Many (WORM) is enabled, data stored in the shared folder cannot be modified or deleted.
- WORM cannot be disabled or modified after folder creation.

   a. Under **WORM Settings**, click **Edit**.

   b. Select **WORM**.

   c. Select one of the following options:

      - **Enterprise**: You can write data to the shared folder, but you cannot modify, delete, or restore data in it. You are allowed to remove the shared folder.
      - **Compliance**: You can write data to the shared folder, but you cannot modify, delete, or restore data in it. You are not allowed to remove the shared folder. To delete data in the folder, you must remove the folder's parent storage pool.

   d. Optional: Specify a data retention period.

8. Optional: Configure advanced settings.

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

Option	Description
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled and 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.
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is installed on the NAS.
Enable access-based share enumeration (ABSE)	When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders.
Enable access-based enumeration (ABE)	When enabled, users can only see the files and folders that they have permission to access.

9. Click **Create**.

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	Modify 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 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.
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.

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.

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

For details, see Shared Folder Permissions.

8. Click **Next**.
   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 appy 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.** Click and select the following: • Traverse folder / execute file • List Folder / read data • Read attributes • Read extended attributes • Create files / write data • Create folder / append data • Write attributes • Write extended attributes • Delete (files only) • Read permission **f.** Click **OK**. **g.** Optional: Add a user to the list of users with permissions for the shared folder. **1.** Click **Add**. The **Add Users** window appears. **2.** Select the following: • Create files / write data • Create folder / append data • Write attributes

Permission Type	Description	User Action
NFS host access	Edit NFS host access rights for shared folders.	**a.** Select **Access right** to enable NFS access rights. **Note** You can't select this for folders mounted by HybridMount using SMB file protocol. These folders do not support NFS host access. However, you can still access the NFS host access page. **b.** 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**.
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
Read Only		Read/Write
Read/Write		Read/Write • Shared folders through Samba/AFP: Read/Write • Shared folders through NFS: Read Only
Not Specified		Read/Write
No Access	Not Specified	No Access
Read Only		Read Only
Read/Write		Read/Write
Not Specified		No Access

Folder Aggregation

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

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

Note

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

Creating a Portal Folder

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

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Folder Aggregation** .
2. Under **Folder Aggregation List**, click **Create a Portal Folder**.
   The **Create a Portal Folder** window appears.
3. Specify the following information.

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

4. Click **Apply**.

Modifying Portal Folder Information

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

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

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

4. Click **Apply**.

Deleting Portal Folders

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

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

Importing Folder Trees

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

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

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

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

Exporting Folder Trees

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

1. Go to **Control Panel** > **Privilege** > **Shared Folders** > **Folder Aggregation** .
2. Click **Import/Export Folder Tree**.
   The **Import/Export Folder Tree** window appears.
3. Under **Export Folder Tree**, click **Export**.
   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.

4. Click **Finish**.

Shared Folder Encryption

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

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.

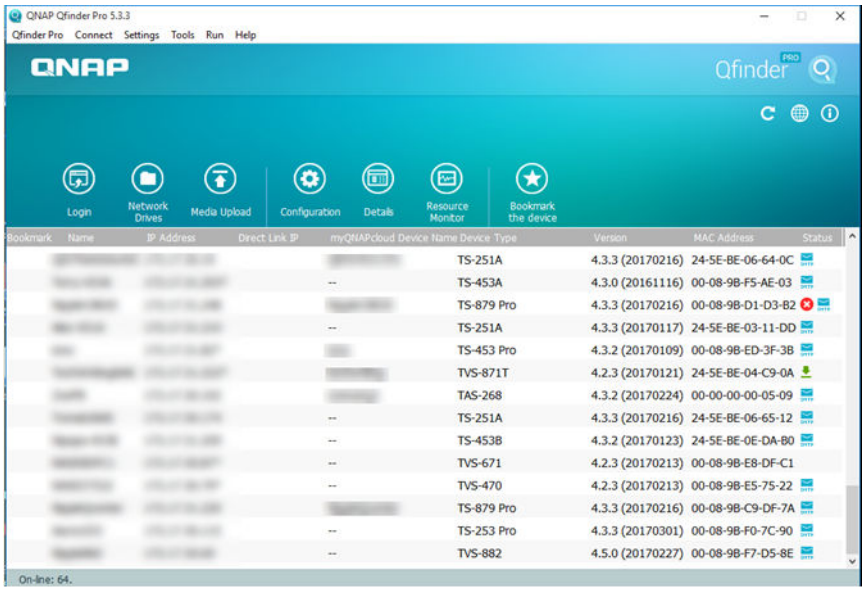
To download Qfinder Pro, go to https://www.qnap.com/utilities.

Mapping a Shared Folder on a Windows Computer

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

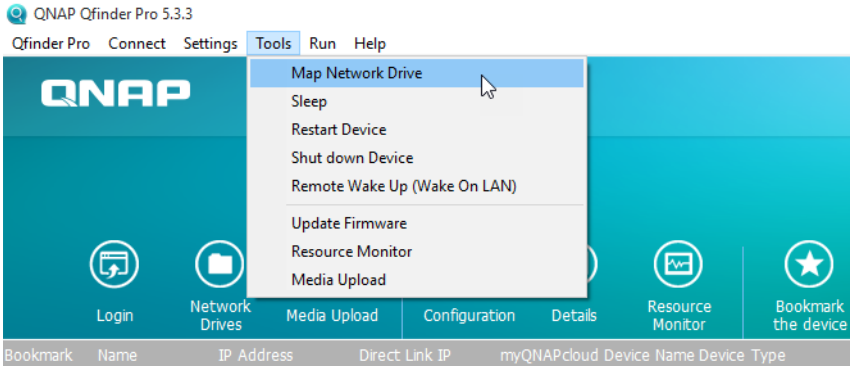
1. Power on the NAS.
2. Connect the NAS to your local area network.

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



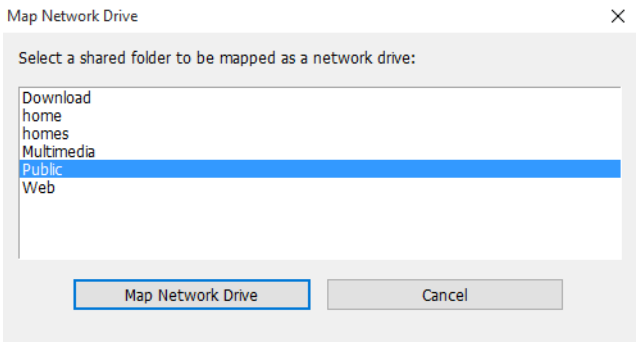
4. Select the NAS where the shared folder is located.

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

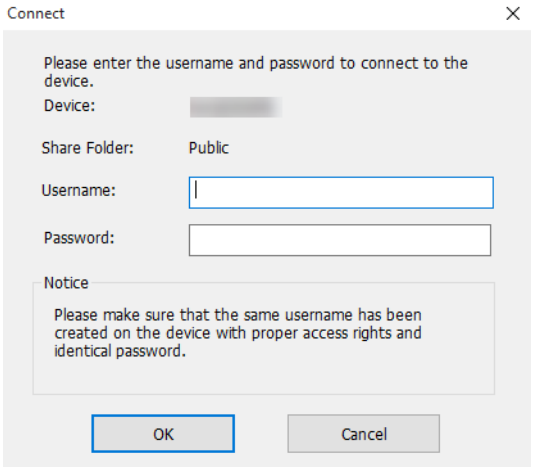


6. Select a shared folder.

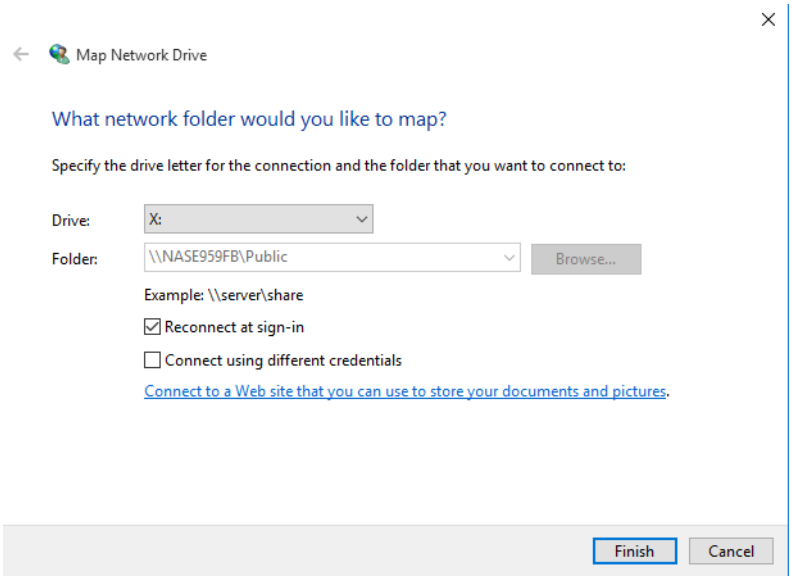
7. Click **Map Network Drive**.



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.

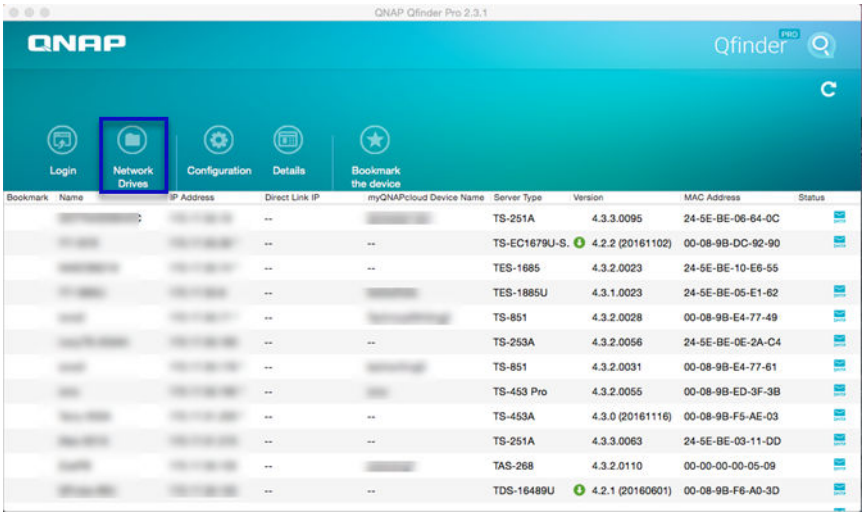
11. Click **Finish**.

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

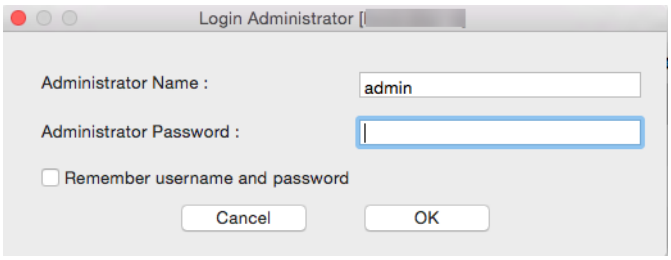
Mounting a Shared Folder on a Mac Computer

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**.

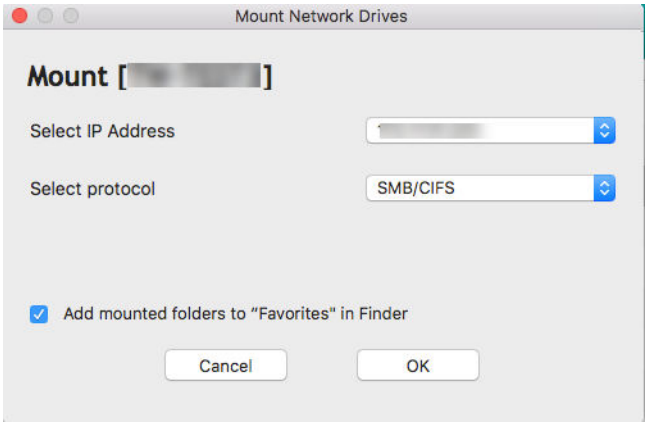


6. Specify your QuTS hero username and password.
7. Click **OK**.



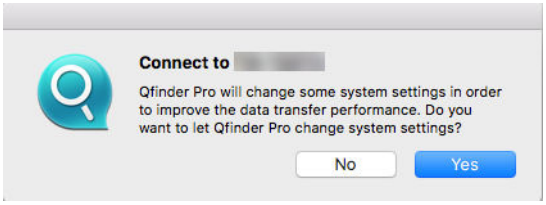
The **Mount Network Drives** window opens.

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

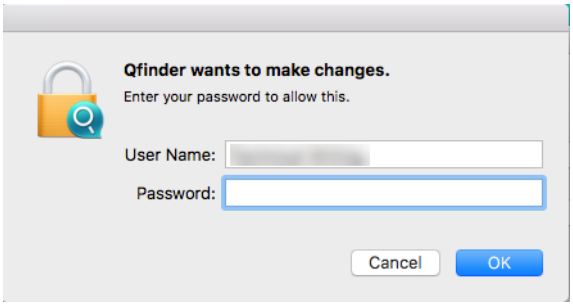


A confirmation message appears.

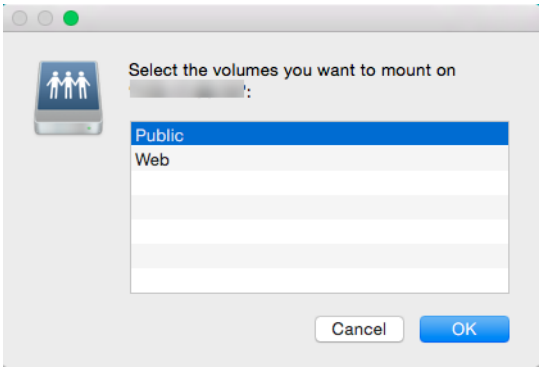
10. Click **Yes**.



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.
   - **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, and 2019.

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

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

Active Directory (AD) Authentication

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

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

Configuring AD Authentication Using the Quick Configuration Wizard

1. Go to **Control Panel** > **Privilege** > **Domain Security** .
2. Select **Active Directory authentication (Domain member)**.
3. Click **Quick Configuration Wizard**.
   The **Active Directory Wizard** appears.
4. Click **Next**.
5. Specify the fully qualified domain name (FQDN) of the AD DNS server.
   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. Select the server signature rule for the domain.

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

11. Specify the domain administrator username and password.
12. Click **Join**.
    The NAS joins the domain.
13. Click **Finish**.

Configuring AD Authentication Manually

Verify the following before starting this task:

- The time settings of the NAS and the AD server are identical. The maximum time disparity tolerated is 5 minutes.
- The AD server is configured as the primary DNS server. If you use an external DNS server, you will not be able to join the domain.
- You have specified the IP address of the WINS server that you use for name resolution.

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

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

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

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

5. Select the server signature rule for the domain.

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

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.

Enabling Trusted Domain Authentication

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

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

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

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

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

Azure Active Directory Single Sign-On (SSO)

Single Sign-On (SSO) is a holistic approach to authenticate users when signing on to applications in Azure Active Directory. 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.

Enabling Azure AD Single-Sign-On

Before starting this task, ensure that you create an application registration. For details, see https://docs.microsoft.com/en-us/azure/active-directory/develop/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://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal.
  You can also add a custom domain name using the Azure AD portal for the on-premise Windows AD. For details, visit https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal and https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain.
- Configure Azure AD Domain service. For details, see the following:
  - Configuring AD Authentication Using the Quick Configuration Wizard
  - Configuring AD Authentication Manually

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

1. Go to **Control Panel** > **Privilege** > **Domain Security** > **SSO** .
2. Select **Enable Azure SSO Service**.
3. Specify **Client ID**.
   For details, visit https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.

Note
The Client ID is also known as an Application ID.

4. Specify **Tenant ID**.
   For details, visit https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.
5. Specify **Reply URLs**.
   a. Sign in as an administrator at https://portal.azure.com/#home.
   b. Click **Azure Active Directory**, and then click **App registrations** > **Your app** > **All settings** > **Reply URLS** .
   c. Add `:8080/cgi-bin` to the end of the IP address.
   d. Copy and paste the URL into the **Reply URLs** field label on the NAS.
6. Specify the **Public key**.

Note

- The public key must be a PEM file.

- You can convert a CA certificate to a public key using a Linux environment or an OpenSSL.

7. Click **Apply**.

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

LDAP Authentication

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

Configuring LDAP Authentication

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

LDAP Server Type	Fields	User Action
Remote LDAP server	**LDAP Server Host**	Specify the host name or IP address of the LDAP server.
	LDAP Security	Select the method that the NAS uses to communicate with the LDAP server. • **ldap://**: Use a standard LDAP connection. The default port is 389. • **ldap:// (ldap + TLS)**: Use an encrypted connection with TLS. The default port is 389. Newer versions of LDAP servers normally use this port. • **ldap:// (ldap + SSL)**: Use an encrypted connection with SSL. The default port is 686. Older versions of LDAP servers normally use this port.
	Base DN	Specify the LDAP domain. Example: `dc=mydomain,dc=local`
	Root DN	Specify the LDAP root user. Example: `cn=admin, dc=mydomain,dc=local`
	Password	Specify the root user password.
	Users Base DN	Specify the Organizational unit (OU) where users are stored. Example: `ou=people,dc=mydomain,dc=local`
	Group Base DN	Specify the OU where groups are stored. Example: `ou=group,dc=mydomain,dc=local`
	Current Samba ID	N/A

LDAP Server Type	Fields	User Action
LDAP server of the remote NAS	**IP address or NAS name**	Specify the server IP address or the name of the NAS.
	LDAP domain	Specify the LDAP domain name.
	Password	Specify the NAS administrator password.
LDAP server of the local NAS	N/A	N/A
IBM Lotus Domino	This server type includes the same fields as **Remote LDAP server**, in addition to the following:	
	uidNumber	Specify the uid number. Select **HASH**.
	gidNumber	Specify the gid number. Select **HASH**.

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.
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.

Task	User Action
Edit shared folder permissions	**a.** Under **Action**, click . The **Edit Shared Folder Permission** window appears. **b.** Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions.

Tip

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

5. Click **Apply**.

Domain Controller

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

Enabling a Domain Controller

Important

When the NAS is configured as a domain controller, only domain users can access shared folders through CIFS/SMB (Microsoft Networking). All local NAS users are denied access. To enable **Domain Controller**, you must first enable Advanced Folder Permissions by going to **Control Panel** > **Privilege** > **Shared Folders** > **Advanced Permissions** .

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

Important

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

3. Select the domain controller mode.

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

4. Specify the following information.

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

5. Select the server signature rule for the domain.

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

6. Click **Apply**.

Resetting a Domain Controller

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

Default Domain User Accounts

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

Creating a Domain User

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

Field	Description
Username	Specify a username between 1 and 20 characters that does not: • Begin with a space • Begin with the following characters: - # @ • Contain the following characters: " + = / \ : | * ? < > ; [ ] % ` '
Password	Specify a password between 8 and 127 characters that contains at least three of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
Description (optional)	Specify a user description that contains a maximum of 1024 ASCII characters.
Email (optional)	Specify an email address that will receive notifications from 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** > **Privilege** > **Domain Controller** > **Users** .
2. Click **Create** > **Create Multiple Users** .
   The **Create Multiple Users** wizard appears.
3. Click **Next**.
4. Specify the following information.

Field	Description
User Name Prefix	Specify a username prefix between 1 and 16 ASCII characters that does not: • Begin with a space • Begin with the following characters: - # @ • Contain the following characters: " + = / \ : | * ? < > ; [ ] % `' This prefix will be included before all usernames.
User Name Start No	Specify a starting number up to 8 digits in length. **Note** 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** > **Privilege** > **Domain Controller** > **Users** .
2. Click **Create** > **Batch Import Users** .
   The **Batch Import Users** wizard appears.
3. Optional: Select **Overwrite existing users**.

Important
When selected, 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** > **Privilege** > **Domain Controller** > **Users** .
2. Locate a user.
3. Perform any of the following tasks.

Task	User Action
Change password	**a.** Under **Action**, click . The **Change Password** window appears. **b.** Specify a password that meets the requirements. **c.** Verify the password. **d.** Click **Change**.
Edit user properties	**a.** Under **Action**, click . The **Edit User Properties** window appears. **b.** Edit the user properties. For details, see Creating a Domain User. **c.** Click **Finish**.
Edit user group membership	**a.** Under **Action**, click . The **Edit User Groups** wizard appears. **b.** Select or deselect user groups. For details, see Domain User Groups. **c.** Click **Next**. **d.** Review the summary, and then click **Finish**.
Edit user profile	**a.** Under **Action**, click . The **Edit User Profile** window appears. **b.** Specify the following: • **Profile path** Specify the shared folder where the roaming profiles are stored. • **Login script** Specify the login script that executes when a domain user logs in from a computer member of the domain. To directly specify the script filename, connect to **\NAS\netlogon** using the domain administrator account and copy the script to the **\sysvol** shared folder in the **\scripts** folder of your domain. • **Home Folder** Specify the drive and shared folder that is mapped to the drive when the domain user logs in to the domain. • Click **Finish**.

Tip
You can also edit quota settings for domain users. For details, see Editing Quota Settings.

Deleting Domain Users

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

Note
The administrator account cannot be deleted.

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

Domain User Groups

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

Default Domain User Groups

- Allowed RODC Password Replication Group
- Certificate Service DCOM Access
- Denied RODC Password Replication Group
- Enterprise Read-Only Domain Controllers
- Incoming Forest Trust Builders
- Network Configuration Operators
- Pre-Windows 2000 Compatible Access
- Read-Only Domain Controllers
- Terminal Server License Servers
- Windows Authorization Access Group

Creating a Domain User Group

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

6. Review the summary, and then click **Finish**.

Editing Domain User Groups

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Groups** .
2. Locate a domain user group.
3. Under **Action**, click .
   The **Edit Group Users** wizard appears.
4. Select or deselect user groups.
5. Click **Next**.
6. Review the summary, and then click **Finish**.

Deleting Domain User Groups

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

Note
Some default user groups cannot be deleted.

Important
Do not delete the default group of the domain.

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

Computers

The **Computers** screen displays the computer accounts for computers or NAS devices that have joined the domain. Computer accounts are created automatically when a computer or NAS joins the domain.

Creating a Computer Account

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Computers** .
2. Click **Create a Computer**.
   The **Create a Computer** wizard appears.
3. Specify the following information.

Field	Description
Computer name	Specify a computer name between 1 and 15 ASCII characters that include any of the following: • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Dashes (-)
Description	Specify a user description that contains a maximum of 1024 ASCII characters.
Location	Specify the location of the computer using a maximum of 1024 ASCII characters.

4. Click **Next**.
5. Assign the account to existing Windows user groups.
6. Click **Next**.
7. Review the summary, and then click **Create**.

Modifying Computer Account Information

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Computers** .
2. Locate a computer account.
3. Perform any of the following tasks.

Task	User Action
Edit computer properties	**a.** Under **Action**, click . The **Edit computer properties** window appears. **b.** Edit the **Description** or **Location**. For details, see Creating a Computer Account.
Edit user group membership	**a.** Under **Action**, click . The **Edit User Groups** window appears. **b.** Select or deselect user groups. For details, see Domain User Groups. **c.** Click **Next**.

4. Click **Finish**.

Editing Computer Account Shared Folder Permissions

1. Go to **Control Panel** > **Privilege** > **Computers** .
2. Locate a computer account.
3. Under **Action**, click .

The **Edit Shared Folder Permission** window appears.

4. Edit the computer account's permissions for each shared folder.
   For details, see Shared Folder Permissions.
5. Click **Apply**.

Deleting Computer Accounts

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

Note
The host computer account cannot be deleted.

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

DNS

The Domain Name System (DNS) helps the domain controller locate services and devices within the domain using service and resource records. Two DNS zones are created by default: the domain created when setting up the NAS as a domain controller, and a zone called "_msdcs". System administrators can modify DNS settings and add or delete domains and records.

Modifying DNS Settings

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **DNS** .
2. Log in under the domain administrator account.

Note
This is the account created when enabling the domain controller.

   a. Specify the following information.

Field	Description
Account	Enter `administrator`.
Password	Enter the password specified when the account was created.

   b. Click **Login**.

3. Under **DNS Settings**, select a domain.
   A list of records appears.
4. Select a record.
   The properties panel appears.
5. Modify any of the following.

Field	Description
Name	Edit the name of the record.

Field	Description
Type	Select the type of record.

6. Modify the values.

Task	User Action
Add a value	**a.** Specify a value. **b.** Click . The value is added to the list.
Move a value up	**a.** Select a value from the list. **b.** Click . The value moves up in the list.
Move a value down	**a.** Select a value from the list. **b.** Click . The value moves down in the list.
Remove a value	**a.** Select a value from the list. **b.** Click . The value is removed from the list.

7. Click **Apply**.

Adding Domains

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **DNS** .
2. Log in under the domain administrator account.

Note
This is the account created when enabling the domain controller.

   a. Specify the following information.

Field	Description
Account	Enter `administrator`.
Password	Enter the password specified when the account was created.

   b. Click **Login**.

3. Click **Action** > **Add Domain** .
   The **Add New Domain** window appears.
4. Enter the domain name.
5. Click **Create**.

Adding Records

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

2. Log in under the domain administrator account.

> **Note**
> This is the account created when enabling the domain controller.

   a. Specify the following information.

Field	Description
Account	Enter `administrator`.
Password	Enter the password specified when the account was created.

   b. Click **Login**.

3. Select a domain or record.

4. Click **Action** > **Add Record** .
   The **Add New Record** window appears.

5. Specify the following information.

Field	Description
Record Name	Specify the name of the record.
Type	Select the type of record.
Value	Specify the value.

6. Click **Create**.

Deleting Domains or Records

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

2. Log in under the domain administrator account.

> **Note**
> This is the account created when enabling the domain controller.

   a. Specify the following information.

Field	Description
Account	Enter `administrator`.
Password	Enter the password specified when the account was created.

   b. Click **Login**.

3. Select a domain or record to delete.

4. Click **Action** > **Delete** .
   A warning message appears.

5. Click **Yes**.

Back Up/Restore

Users can back up or restore domain controller settings. Only the primary domain controller needs to be backed up; backing up the primary domain controller also backs up any additional or read-only domain controllers. When restoring a domain controller, there are some restrictions and limitations if the domain controller is in an AD environment with more than one domain controller. For details, see Restoring Domain Controllers.

Backing Up Domain Controllers

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Backup/Restore** .
2. Under **Back up ADDC Database**, select **Back up Database**.
3. Specify the following information.

Option	Description
Backup frequency	Select how often the Active Directory Domain Controller (ADDC) database is backed up.
Start Time	Select when the backup will begin.
Destination folder	Select the NAS folder where the backup will be stored.
Backup Options	Select one of the following: • **Overwrite existing backup file (dc_backup.exp)** • **Create a new file for each backup and append the date to the filename (dc_backupyyyy_mm_dd_exp)**

4. Click **Apply**.

Restoring Domain Controllers

Important
Restoring a domain controller overwrites all user, user group, and domain controller settings. Any changes made after the backup file was created will be lost.

Warning
Restoring a domain controller in a multiple-controller environment from a backup file will corrupt the domain controller database. Instead, re-add the NAS as a domain controller, and it will synchronize with the existing controller.

1. Go to **Control Panel** > **Privilege** > **Domain Controller** > **Backup/Restore** .
2. Under **Restore ADDC Database**, click **Browse**.
3. Locate a domain controller backup file.
4. Click **Import**.

4. 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

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Overview** .
3. Select **Enable antivirus**.
4. Optional: Under **Update**, enter a check for updates automatically frequency.

Tip

- To update the antivirus now, click **Update now**.
- To manually update the antivirus, click **Browse** and then select an updated file and click **Open**. After the file appears in the text box, click **Import**. You can download updated files from http://www.clamav.net/.

5. Click **Apply**.
   QuTS hero enables the 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 a file filter option.

Tip

- If you select **Quick scan (Only potentially dangerous file types listed below)**, you can manually delete or modify file types.
- If you select **Exclude files or folders**, you can manually type in folder or file names.

10. Click **Next**.
    The **Scan Options** screen appears.
11. Enter a maximum file size that Antivirus can scan.

Note
Antivirus will not scan any file size higher than the specified number.

12. Optional: Select at least one of the following options.

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

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

Option	Description
Only report the virus	QuTS hero reports the virus but does not take any action on the detected files. The detections will appear in **Reports**.
Move infected files to quarantine	QuTS hero quarantines the infected files. You cannot access these files from their shared folders. You can review the virus scan report in **Reports** and delete or restore infected files in **Quarantine**.
Delete infected files automatically	QuTS hero deletes the infected files. **Important** These files are permanently deleted.

15. Click **Finish**.
    The scan job appears underneath **Job Name**.

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. Under **Action**, 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.** Select the option you want to modify. **c.** After modifying the settings, 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	Select . 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. Locate the scan job you want to manage.
4. Under **Action**, 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 logs from all jobs, click **Download All Logs** at the lower right-hand corner of the screen.
Delete	**a.** Select . A confirmation message appears. **b.** Click **Yes**. QuTS hero deletes the scan job.

Note

- You can keep logs for a specified number of days. For **Number of days to keep the logs**, enter a number between 1-999, and then click **Apply**.
- To archive expired logs, select **Archive logs after expiration**, specify the archive folder, and then click **Apply**.

Managing Quarantine Files

Warning
You cannot recover deleted quarantine files.

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel** > **Applications** > **Antivirus** > **Quarantine** .
3. Locate the file you want to manage.
4. Under **Action**, select one of the following options.

Option	User Action
Delete	Click . QuTS hero permanently deletes the file. **Tip** • You can delete multiple files on the list. Select the files you want to delete, and then click **Delete Selected Files**. • You can delete all of the files on the list. To do so, click **Delete All Files**.
Restore	Click . QuTS hero restores the file to its shared folder. **Tip** You can restore multiple files on the list. Select the files you want to restore, and at the top of the screen, select **Restore Selected Files**.
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 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 following settings.

Setting	User Action
Enable HTTP compression	Select this option to improve transfer speeds and bandwidth utilization. **Warning** Enabling this option may lead to security risks.
Enable secure connection (HTTPS)	Select this option to allow HTTPS connections. **a.** Select **Enable secure connection (HTTPS)**. **b.** Optional: Select a TLS version. **Warning** Selecting the latest TLS version may decrease compatibility for other clients in your system. **c.** Specify a port number. **d.** Optional: Select **Force secure connection (HTTPS) only** to require all users to connect to the NAS using only HTTPS.
Maximum number of clients	Enter a maximum client number. **Note** A client number is the number of users that are allowed to connect to the server.
Do not allow Web Server embedding in IFrames	**a.** Select **Do not allow Web Server embedding in IFrames**. **b.** Optional: Add a website to allow Web Server embedding in IFrames. **1.** Click **Allowed Websites**. The **Allowed Websites** window appears. **2.** Click **Add** to add a website to the list. The **Add Host Name** window appears. **3.** Specify a host name. **4.** Click **Add**. The host name is added to the allowed websites list. **5.** Click **Apply**.

Setting	User Action
Enable X-Content-Type-Options HTTP header	Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities.
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.

5. Click **Apply**.

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

QuTS hero enables web server.

Modifying the php.ini Maintenance File

This task requires that you 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. Underneath **php.ini Maintenance**, select one of the following options.

Option	User Action
Upload	**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.
Edit	**a.** Click **Edit**. The **Edit php.ini** window opens. **b.** Edit the php.ini file. **c.** Click **Apply**. QuTS hero saves the changes.
Restore	**a.** Click **Restore**. A confirmation message appears. **b.** Click **OK**. QuTS hero restores the default php.ini file.

Enabling and Creating a Virtual Host

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.

Enabling WebDAV

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel** > **Applications** > **Web Server** > **WebDAV** .
3. Select **Enable WebDAV**.
4. Select one of the following options.
   - **Shared folder permission**
   - **WebDAV permission**
5. Optional: Select **Use dedicated port for WebDAV service**, and then select one of the following options and enter the port number.
   - **HTTP port number**
   - **HTTPS port number**
6. Click **Apply**.
   QuTS hero enables WebDAV.

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 Enabling WebDAV.

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 are unable to connect to this shared folder via WebDAV, you may need to modify the basic authentication level in Registry Editor. Right-click **Start** and select **Run**. Type `regedit` and click **OK**. In Registry Editor, go to **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **WebClient** > **Parameters** . Open **BasicAuthLevel** and set the value data to `2`. Restart your computer and try connecting to the shared folder using WebDAV again.

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.

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 Enabling WebDAV.

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.

Enabling 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. Enter and verify the password.
6. Click **Apply**.

SQL Server

You can use the SQL Server to turn your NAS to a website database.

Enabling SQL Server

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel** > **Applications** > **SQL server** .
3. Optional: Change your SQL server password.

Important
To prevent security risks, you cannot enable SQL server if the SQL server password is `admin` or blank.

   a. Underneath **Database Maintenance**, select **Change Root Password**.
   The **Change Root Password** window opens.
   b. Enter the new password twice.
   c. Click **OK**.
   QuTS hero changes the root password and a confirmation window opens.
   d. Click **OK**.

4. Select **Enable SQL server**.
5. Optional: Enable TCP/IP networking.

Tip
If you do not enable this option, the SQL Server is only configured as a local database server. Enable this option if you want to configure the SQL Server to be used as another web server on the network.

   a. Select **Enable TCP/IP networking**.
   b. Enter a port number.

Note
The default port is 3306.

6. Click **Apply**.
   QuTS hero enables SQL server.

Reinitializing the Database

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel** > **Applications** > **SQL server** .
3. Underneath **Database Maintenance**, click **Reinitialize Database**.
   The **Reinitialize Database** window opens.

4. Enter and confirm your SQL password.
5. Click **Reinitialize**.
   QuTS hero reinitializes the database and a confirmation message appears.
6. Click **OK**.

Syslog Server

You can configure the NAS as a Syslog Server. This allows you to collect various device logs from different machines in one location.

Enabling 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. Select at least one of the following options.

Option	User Action
Enable TCP	**a.** Select **Enable TCP**. **b.** Enter a TCP port.
Enable UDP	**a.** Select **Enable UDP**. **b.** Enter a UDP port.

5. Optional: Configure the log settings.
   a. Underneath **Log Settings**, enter a number between 1-100 to specify the maximum log size.
   b. Select the destination folder where you want to save the logs.
   c. Enter the log file name.
6. 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**
      - **not starts with**
      - **not contains**
   c. Enter the filter condition.
   d. Click **Add**.

Tip

- To remove an existing filter, click **Remove**.
- To manually edit a filter, select **Manual Edit**.

   e. 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. Under **Action**, select one of the following options.

Option	User Action
Enabled **Note** This option only appears for disabled filters.	Click . QuTS hero enables the filter.
Disabled **Note** This option only appears for enabled filters.	Click . QuTS hero disables the filter.
Edit	**a.** Click . The **Filter** window opens. **b.** Modify the filter. **c.** Click **Apply**. QuTS hero saves the filter information.

Tip

- To delete a filter, select a filter from the list, click **Delete**, and then **Yes**.
- To view Syslogs, go to **Control Panel** > **Applications** > **Syslog Server** > **Syslog Viewer** .

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 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. Under **Action**, select one of the following options.

Option	User Action
Enabled	Click . QuTS hero enables the client.
Disabled	Click . QuTS hero disables the client.
Edit	**a.** Click . The **Edit Client** window opens. **b.** Configure the client information. **c.** Click **Apply**. QuTS hero saves the client information.

Tip
To delete a client, select at least one client, click **Delete**, and then **Yes**.

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. Under **Action**, select one of the following options.

Option	User Action
Enabled	Click . QuTS hero enables the user.
Disabled	Click . QuTS hero disables the user.
Change Password	**a.** Click . The **Edit User** window opens. **b.** Modify the settings. **c.** Click **Apply**. QuTS hero saves the new password.

Tip
To delete users, select at least one user, click **Delete**, and then **Yes**.

Enabling 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. Enter 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 log file. QNAP recommends viewing the log file using Microsoft Excel or WordPad on Windows or TextEdit on macOS.

   a. Select **Enable TFTP logging**.
   b. Specify the folder where you want to save log files.
   c. Specify the access right.

7. Select where to allow TFTP access.
8. Click **Apply**.

Enabling NTP Server

This task allows the NTP Server to allow 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 NTP Server.

5. File Station

Overview

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
Java program	Java Runtime Environment (JRE) 7 or later
Flash player	Adobe Flash Player 9 or later is required for viewing media files.

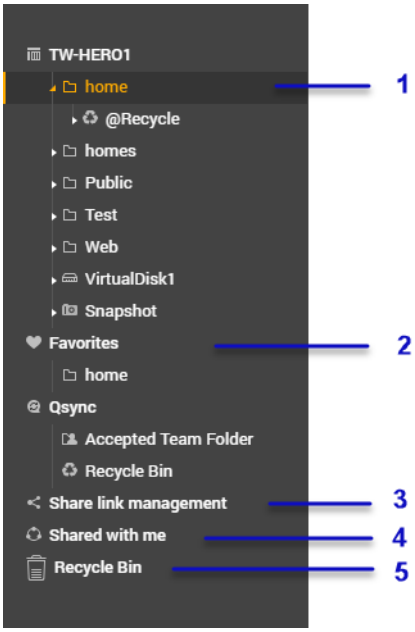
Supported File Formats

Category	File Extension
Image	• BMP • JPG • JPE • PNG • TGA • GIF • HEIC • HEIF
Music	• MP3 • FLAC • OGG • WAV • AIF • AIFF

Category	File Extension
Video	• AVI • MP4

Parts of the User Interface

Left Panel



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

Depending on your setup, the following folders may also appear on the list.

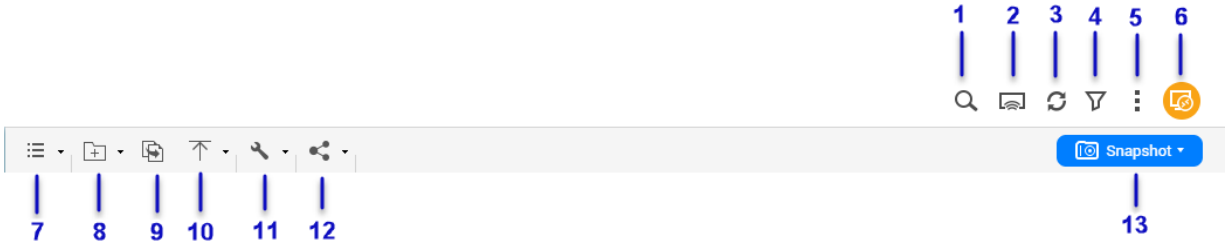
Folder	Description
Snapshot	Displays the saved snapshots.

Folder	Description
Local folders	Displays the local folders on a Windows computer. **Important** To view local folders from File Station, you must first install Java Runtime Environment.
Qsync	Displays files, folders, and team folders from Qsync.
VJBOD Cloud shared folder	Displays files and folders from a shared folder created on a VJBOD Cloud Volume. **Note** To view the folder name, capacity, amount of free space available, and the storage pool, hover your cursor over a VJBOD Cloud shared folder.

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.
SFTP	Displays a list of connections mounted through a Secure File Transfer Protocol (SFTP).

Toolbar



Label	Item	Description
1	Search	Search files and folders by their name or type. **Tip** You can select **Advanced Search** to specify more criteria.
2	Network Media Player	Stream videos, photos, and music to compatible devices on your network.
3	Refresh	Refresh the current page.
4	Smart Filter	Filter files and folders based on the specified criteria.
5	More Settings	Configure File Station settings, open the Help guide, or view application information.

Label	Item	Description
6	Remote Mount	Manage files across local, external, remote, and cloud storage resources on a single interface. To use this feature, install HybridMount from App Center. For more information on HybridMount, go to the QNAP website.
7	Browsing Mode	Select a browsing mode.
8	Create folder	Create a folder, shared folder, or share a space with another NAS user.
9	Copy	Copy the selected files and folders. **Note** This button only appears when a file or folder is selected.
10	Upload	Upload files or folders to the selected shared folder.
11	More Actions	Perform different tasks. **Note** Some task options only appear when you select certain types of files.
12	Share	Share the selected files and folders. **Note** This button only appears when a file or folder is selected.
13	Snapshot	Open Snapshot Manager or view the Snapshot Manager quick tutorial.

Settings

Modifying General Settings

1. Click ⋮ on the top-right corner.
2. Select **Settings**.
   The **Options** window appears.
3. Select **General**.
4. 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 Network Recycle Bin(s)	File Station displays the `@Recycle` folder in all user folders.
Only allow the admin and administrators group to use "Share to NAS user"	File Station prevents non-administrators from sharing files with other NAS users.
Only allow the admin and administrators group to permanently delete files	File Station prevents non-administrators from permanently deleting files.
Only allow the admin and administrators group to use on-the-fly transcode	File Station prevents non-administrators from using on-the-fly transcoding.

Option	Description
Track file and folder access	File Station allows users to track file or folder access and view information in System Access Logs.

5. Click **Close**.

Modifying File Transfer Settings

1. Click ⋮ on the top-right corner.
2. Select **Settings**.
   The **Options** window appears.
3. Select **File Transfer**.
4. 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**

5. Optional: Select **Always merge all file transfer processes into one task**.
6. 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

7. Click **Apply**.
8. Click **Close**.

Modifying Multimedia Settings

1. Open File Station.

2. Click ⋮ on the toolbar.
3. Select **Settings**.
   The **Options** window appears.
4. Select **Multimedia**.
5. Modify the following settings.

Option	Description
Support multimedia playback and thumbnail display	File Station allows multimedia playback and displays thumbnails for media files.
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. Click ⋮ on the top-right corner.
2. Select **Settings**.
   The **Options** window appears.
3. Select **Documents**.
4. Optional: Select **Support PDF thumbnail display**.

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

5. 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

6. 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.

7. Click **Apply**.
8. 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.

1. Click ⋮ on the top-right corner.
2. Select **Settings**.
   The **Options** window appears.
3. Select **Third-party Service**.
4. Acquire your CloudConvert API key.

> **Tip**
> For details, see the tutorial: https://www.qnap.com/en/how-to/faq/article/how-to-get-an-api-key-from-cloudconvert

5. Paste your CloudConvert API key.
6. Click **Apply**.

File Operations

File Station enables you to perform the following tasks.

Operation	Task
Store	• Uploading a File
Access	• Downloading a File • Opening a File • Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension • Opening a Text File Using Text Editor • Viewing a File in Google Docs • Viewing a File in Microsoft Office Online • Opening Image Files Using Image2PDF • Viewing File Properties • Modifying File Permissions

Operation	Task
Organize	• Sorting Files • Copying a File • Moving a File • Renaming a File • Deleting a File • Restoring a Deleted File • Mounting an ISO File • Unmounting an ISO File • Compressing a File • Extracting Compressed Files or Folders
Share	• Sharing a File or Folder by Email • Sharing a File or Folder on a Social Network • Sharing a File or Folder Using Share Links • Sharing a File or Folder with a NAS User
Play	• Playing an Audio File • Playing a Video File • Opening a 360-degree Image or Video File • Streaming to a Network Media Player
Transcode	• Adding a File to the Transcoding Folder • Canceling or Deleting Transcoding • Viewing Transcode Information

Uploading a File

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

Method	Steps
Using the toolbar	**a.** Click and then select **File**. The **File Upload** window opens. **b.** Select the file and then click **Open**.
Using drag and drop	**a.** Locate the file on your computer. **b.** Drag and drop the file to the File Station window.

A confirmation message appears.

3. Select one of the following policies for handling duplicate files.

Option	Description
Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.

Tip
You can set the selected option as the default policy. File Station will not ask again after remembering the setting. You can still change the policy in **File Station** > **More Settings** > **Settings** > **File Transfer** .

4. Click **OK**.
File Station uploads the file.

Downloading a File

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

Method	Steps
Using the toolbar	a. Select the file. b. Click . c. Select **Download**. d. Click **OK**.
Using the context menu	Right-click the file and then click **Download**.

Depending on your browser, a confirmation message appears before the file is downloaded to your computer.

Opening a File

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

Method	Steps
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**

File Station opens the selected file.

Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension

This task requires that you use the Google Chrome browser and install the Office Editing for Docs, Sheets & Slides extension.

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Select **Open with Chrome Extension**.
Using the context menu	Right-click the file and then select **Open with Chrome Extension**.

File Station opens an editable file on Google Docs, Sheets, or Slides.

Opening a Text File Using Text Editor

This task requires that you install Text Editor from the App Center.

1. Open File Station.

2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Select **Open with Text Editor**.
Using the context menu	**a.** Right-click the file. **b.** Select **Open with Text Editor**.

File Station opens the selected text file using Text Editor.

Viewing a File in Google Docs

This task requires that you use the Google Chrome browser and enable myQNAPcloud Link.

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

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

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

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

Viewing a File in Microsoft Office Online

This task requires that you enable myQNAPcloud Link.

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

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

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

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

File Station opens the file in Microsoft Office Online.

Opening Image Files Using Image2PDF

You must to install Image2PDF from the App Center before starting this task.

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

Method	Steps
Use the menu bar	**a.** Select the file. **b.** Click . **c.** Select **Open with Image2PDF**.
Use the context menu	Right-click and then select **Open with Image2PDF**.

File Station opens the selected image file with the Image2PDF wizard.

Follow the wizard's on-screen instructions to convert the image file into a PDF file.

Viewing 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
Type	Displays the file type.
Size	Displays the file size.
File Path	Displays the folder location.
Modified Date	Displays the date that the file was last modified.
Owner	Displays name of the NAS user who uploaded the file.
Group	Displays the name of the NAS group that can access the file.
Storage Pool	Displays the name of the storage pool on which the file is located.
View Access Logs	Keeps track of access to the file. **Tip** You can view access logs in QuLog Center.

4. Click **Close**.

Modifying File Permissions

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.

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

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

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

6. Optional: Select the access rights for guest users.

7. Optional: Specify the ownership of the file.
   a. Click .
   b. Select a user.
   c. Click **Set**.
8. Click **Apply**.

Sorting Files

1. Open File Station.
2. Locate the folder.
3. Click .
4. Select **List**.
   File Station displays files in a list view.
5. Click a column title.
   File Station sorts files in an ascending or descending order based on the selected column.

Tip
You can manually adjust column widths, except for **Name**. To manually adjust the column width, click and drag the end of the column name.

Copying 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 **Copy to/Move to** and then select **Copy to**. d. Select the destination folder. e. Click **OK**.
Using the context menu	a. Right-click the file. b. Select **Copy**. c. Go to the destination folder. d. Right-click inside the folder and then select **Paste**.

Method	Steps
Using keyboard shortcuts	**a.** Select the file. **b.** Press **CTRL + C** or **Command-C**. **c.** Go to the destination folder. **d.** Press **CTRL + V** or **Command-V**.
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 • Copy and overwrite • Copy and rename automatically

File Station creates a copy of the selected file.

Moving a File

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Select **Copy to/Move to** and then select **Move to**. **d.** Select the destination folder. **e.** Click **OK**.
	a. Select the file. **b.** Click . **c.** Select **Cut**. **d.** Select the destination folder. **e.** Click . **f.** Select **Paste**.

Method	Steps
Using the context menu	**a.** Right-click the file and then select **Copy to/Move to** and **Move to**. **b.** Select the destination folder. **c.** Click **OK**.
	a. Right-click the file and then select **Cut**. **b.** Select the destination folder. **c.** Right-click inside the folder and then select **Paste**.
Using keyboard shortcuts	**a.** Select the file. **b.** Press **CTRL + X** or **Command-X**. **c.** Go to the destination folder. **d.** Press **CTRL + V** or **Command-V**.
Using drag and drop	**a.** Select the file. **b.** Drag and drop to the destination folder. **c.** Step result: A context menu appears. **d.** Select one of the following actions. • Move and skip • Move and overwrite • Move (and rename if a file exists with the same name)

File Station moves the selected file to the specified folder.

Renaming a File

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Select **Rename**.
Using the context menu	**a.** Right-click the file. **b.** Select **Rename**.
Use a keyboard shortcut	Press **F2**.

4. Specify the file name and then click **OK**.
File Station renames the file.

Deleting a File

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

Method	Steps
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 Network Recycle Bin
   - Delete permanently
5. Click **OK**.
   File Station either moves the selected file to the Recycle Bin or deletes it permanently.

Restoring a Deleted File

1. Open File Station.
2. Go to **Recycle Bin**.
3. Locate the file.
4. Perform one of the following methods.

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

   A confirmation message appears.

5. Click **Yes**.

File Station restores the selected file.

Mounting an ISO File

1. Open File Station.
2. Upload an ISO file.
   For details, see Uploading a File.
3. Perform one of the following methods.

Method	Steps
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**.

Compressing a File

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

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

4. Configure the file compression settings.

Option	Task
Archive name	Specify a name for the compressed file.
Compression level	Select the type of compression method. • **Normal** - Standard compression • **Maximum compression** - Prioritizes compression quality • **Fast compression** - Prioritizes compression speed
Archive format	Select the format of file compression. • **zip** • **7z**
Update mode	Specify how the files should be updated. • **Add and replace files** • **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 file and creates a archive file.

Sharing a File or Folder by Email

Before starting this task, you must configure the QuTS hero email settings in **Desktop** > > **E-mail Account** .

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

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

The **Share** window appears.

4. Configure the following settings.

Field	User Action
Send from	Select the email delivery method. • Use NAS to mail the links. • Use local computer to mail the links.
Sender	Select an email account.
To	Specify the email address of the recipient. **Tip** You can select a recipient from your contact list if Qcontactz is installed on the NAS.
Subject	Specify the email subject line.
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Enter a name for the link or use the current name of the file or folder. **Note** A link name cannot contain the following characters: / | \ : ? < > * "

Field	User Action
Domain name/IP	Select the domain name or IP address. **Tip** The following domains and IP addresses are supported: • **myQNAPcloud**: Provides a link to the shared file or folder using the DDNS address set in myQNAPcloud. • **WAN**: Provides a link to the shared file or folder to other computers using a different network. • **LAN**: Provides a link to the shared file or folder to other computers using the same local network. • **SmartShare**: Provides a SmartURL via myQNAPcloud Link to the shared file or folder. • **All available links**: Provides links to the shared file or folder using all of the available domains and IPs. **Note** The recipients get direct read access.
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	Allow users to transcode videos on the fly. **Note** • This setting only appears when sharing files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	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. **Tip** To include the password in the email, select **Show the password in the email**.

6. Click **Share Now**.
   File Station sends an email to the recipient.

Sharing a File or Folder on a Social Network

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

Method	User Action
Using the toolbar	**a.** Select the file or folder. **b.** Click **Share**. **c.** Select **To Social Network**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** and then select **To Social Network**.

The **Share** window appears.

4. Configure the following settings.

Field	User Action
Social Network	Select the social network website.
Message	Enter a new message or use the default message.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Type a name for the link or use the current file or folder name. **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 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 video files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder **Note** This setting only appears when 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 **Share**. **c.** Select **Create share link only**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** and then select **Create share link only**.

The **Share** window appears.

4. Configure the following settings.

Field	User Action
Link Name	Type a name for the link or use the current file or folder name. **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 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 video files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).

Field	User Action
File upload	Allow users to upload files to this folder **Note** This setting only appears when sharing folders.
Expire in	Specify the expiration date. **Note** This setting only appears when you share a folder.
Password	Require a password to access the link.

5. Click **Create Now**.
   File Station generates a link.

Sharing a File or Folder with a NAS User

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

Method	User Action
Using the toolbar	**a.** Select the file or folder. **b.** Click **Share**. **c.** Select **To NAS user**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Share** and then select **To NAS user**.

   The **Share** window appears.

4. Select the user to share the file or folder with.

Option	User Action
Existing user	Select a user from the list. Optional: Select **Send a notification email to the user** and then specify the email subject and message. Only users who have provided email information will receive notifications. **Note** You can specify the email information of each user in **Control Panel** > **Privilege** > **Users** .
New user	Create a new user account.

5. Optional: Click **More settings** and configure additional settings.

Field	User Action
Link Name	Type a name for the link or use the current file or folder name. **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 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 video files. • To use on-the-fly transcoding, you must install and enable Video Station 5.2.0 (or later).
File upload	Allow users to upload files to this folder **Note** This setting only appears when sharing folders.
Expire in	Specify the expiration date. **Note** You cannot access the shared file or folder after the expiration date.

Field	User Action
Password	Enable to specify a password to access the link. **Note** If you enable this option, this field cannot be empty. **Tip** To include the password, select **Show the password in the email**.

6. Click **Share Now**.
   File Station shares the file with the specified user.

Playing an Audio File

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

Method	Steps
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

You must install Video Station from App Center to play certain video formats.

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Select **Play**. **d.** Select a resolution.
Using the context menu	**a.** Right-click the file.

	b. Select **Play**. **c.** Select a resolution.

File Station plays the selected file using Media Viewer.

Playing a Video File Using CAYIN MediaSign Player

CAYIN MediaSign Player is a third-party web media player. You must install CAYIN MediaSign Player from App Center and have an activated license to play video files.

Note
CAYIN MediaSign Player can be enabled and disabled using Multimedia Services.

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click . **c.** Click **Play with CAYIN MediaSign Player**.
Using the context menu	**a.** Right-click the file. **b.** Click **Play with CAYIN MediaSign Player**

File Station plays the selected file using CAYIN MediaSign Player.

Opening a 360-degree Image or Video File

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

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

4. Optional: Select the resolution.

File Station opens the selected file using the Media Viewer. You can click **360 Panorama Mode** ( ) on Media Viewer to view the photo or video in Panorama Mode.

Streaming to a Network Media Player

This task requires that you install Media Streaming Add-on from App Center.

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

Method	Steps
Using the toolbar	**a.** Select the file. **b.** Click on the toolbar. **c.** Select a media player. The **Media Viewer** window appears. **d.** Select **Play the selected item on this player**. **e.** Click **OK**.
	a. Select the file. **b.** Click . **c.** Hover the mouse pointer over **Streaming to**. **d.** Under **Network Media Player**, select a media player.
Using the context menu	**a.** Right-click the file. **b.** Hover the mouse pointer over **Streaming to**. **c.** Under **Network Media Player**, select a media player.

File Station plays the selected file using the specified network media player.

Adding a File to the Transcoding Folder

Important

- Video files cannot be converted to a resolution higher than the original. If a higher resolution is selected, File Station automatically transcodes the file in its original resolution.
- This task requires transcoding to be enabled on the Multimedia Console.

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.

Extracting Compressed Files or Folders

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

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

4. Select one of the following file extraction options.

Option	Description
Extract files	Select specific files to extract.
Extract here	Extracts all files in the current folder.
Extract to /<new folder>/	Extract all files in a new folder. The new folder uses the file name of the compressed file.

File Station extracts the compressed files to the specified folder.

Folder Operations

File Station enables you to perform the following tasks.

Operation	Task
Store	• Uploading a Folder • Uploading a Folder Using Drag and Drop
Access	• Viewing Folder Properties • Viewing Storage Information • Modifying Folder Permissions • Viewing Qsync Folders • Managing Share Links • Viewing Files and Folders Shared with Me
Organize	• Creating a Folder • Copying a Folder • Creating a Desktop Shortcut • Adding a Folder to Favorites • Removing a Folder from Favorites • Compressing a Folder
Share	• Creating a Shared Folder • Sharing Space with a New User
Transcoding	• Adding a Folder to the Transcoding Folder • Canceling or Deleting Transcoding

Uploading a Folder

Note
This feature is only available on Google Chrome browsers.

1. Open File Station.
2. Open the destination folder.
3. Click and then select **Folder**.
   The **Browse for Folder** window opens.
4. Select the folder to upload.
   A confirmation message appears.
5. Select one of the following policies for handling duplicate files.

Option	Description

Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.

Tip
You can set the selected option as the default policy. File Station will not ask again after remembering the setting. You can change the policy later in **File Station** > **More Settings** > **Settings** > **File Transfer** .

6. Click **OK**.
   File Station uploads the selected folder.

Uploading a Folder Using Drag and Drop

Note
This feature is only available on Google Chrome browsers.

1. Open File Station.
2. Drag and drop the local folder to File Station.
3. Select one of the following policies for handling duplicate files.

Option	Description
Rename duplicate files	Upload and rename a file if another file with the same name and extension already exists in the destination folder.
Skip duplicate files	Do not upload a file if another file with the same file name and extension already exists in the destination folder.
Overwrite duplicate files	Upload the file and then overwrite an existing file with the same name and extension in the destination folder.

4. Click **OK**.
   File Station uploads the selected folder.

Viewing Folder Properties

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 **Properties**.

Method	Steps
Using the context menu	**a.** Right-click the folder. **b.** Select **Properties**.
Use the left panel	**a.** Right-click the folder. **b.** Select **Properties**.

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

Field	Description
Selected items	Displays how many items are selected.
Type	Displays the folder type.
Size	Click to display the folder size and total file count.
File Path	Displays the folder location.
Modified Date	Displays the date that the folder was last modified.
Owner	Displays name of the NAS user who uploaded the folder.
Group	Displays the name of the NAS group that can access the folder.
Storage Pool	Displays the name of the storage pool on which the folder is stored.
WORM	Indicates whether the Write Once Read Many (WORM) feature is enabled for this shared folder.
Compression	Indicates whether compression is enabled for this shared folder.
Deduplication	Indicates whether deduplication is enabled for this shared folder.
SSD cache	Indicates whether SSD cache is enabled for this shared folder.
Fast clone	Indicates whether fast clone is enabled for this shared folder.
View Access Logs	Keeps track of access to the folder. **Tip** To enable this feature, select **Track file and folder access** in **File Station** > **Options** .
Multimedia Console	Opens Multimedia Console. This allows you to manage multimedia content sources.
Shared Folder	Edits folder properties.
Storage Settings	Opens Storage & Snapshots. This allows you configure storage settings for this shared folder.

4. Click **Close**.

Viewing Storage Information

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 **Storage Info**.
Using the context menu	**a.** Right-click the folder. **b.** Select **Storage Info**.

The **Storage Info** window opens and displays the following information.

Information	Description
Shared folder	Displays the names of shared folders.
Used size	Displays the total storage size currently in use.
Capacity	Displays the total storage capacity of the shared folder.
Free size	Displays the total available storage space in the shared folder.

4. Click **Close**.

Modifying Folder Permissions

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

The **Properties** window opens.

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

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

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

6. Optional: Select the access right for guest users.
7. Optional: Specify the ownership of the folder.
   a. Click .
   b. Select a user.
   c. Click **Set**.
8. Optional: Enable one or more of the following settings.
   - Only the owner can delete the contents
   - Only admin can create files and folders
   - Apply changes to files and subfolders
   - Apply and replace all existing permissions
9. Click **Apply**.

Viewing Qsync Folders

1. Open File Station.
2. On the left panel, click **Qsync**.
   File Station displays the list of team folders shared by other NAS users.

Managing Share Links

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

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

Note

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

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

Task	User Action
Re-share	Click and then select one of the following share methods. • Share By Email. • Share on a social network • Use share links • Share with a NAS user
Stop sharing	Click .
Copy the link to the clipboard	Click .

File Station performs the specified task.

Viewing Files and Folders Shared with Me

1. Open File Station.
2. On the left panel, click **Shared with me**.

File Station lists the files and folders shared with the current account. You can copy, open, or download a selected file or folder.

Creating a Folder

1. Open File Station.
2. Locate the destination folder.
3. Perform one of the following tasks.

Task	Steps
Using the toolbar	**a.** Click **b.** Select **Folder**. The **Create folder** window opens. **c.** Specify the folder name. **d.** Click **OK**.
Using the context menu	**a.** Right-click inside the folder and then select **Create folder**. **b.** Specify the folder name. **c.** Click **OK**.

File Station creates a new folder.

Copying a Folder

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 **Copy to/Move to** and then select **Copy to**. **d.** Select the destination folder. **e.** Click **OK**.
Using the context menu	**a.** Right-click the folder. **b.** Select **Copy**. **c.** Go to the destination folder. **d.** Right-click inside the folder and then select **Paste**.

File Station creates a copy of the selected folder.

Creating a Desktop Shortcut

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

Method	Steps
Using the toolbar	**a.** Select the folder. **b.** Click . **c.** Select **Create Shortcut to Desktop**.
Using the context menu	**a.** Right-click the folder. **b.** Select **Create Shortcut to Desktop**.
Drag and Drop	**a.** Select the folder. **b.** Drag and drop the folder to the desktop.

File Station creates a desktop shortcut for the selected folder.

Tip
Hovering the mouse pointer over a desktop shortcut displays the path of the original folder.

Adding a Folder to Favorites

1. Open File Station.

2. Locate the folder.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	a. Select the folder. b. Click . c. Select **Add to Favorites**.
Using the context menu	a. Right-click the folder. b. Select **Add to Favorites**.
Use the Favorites button	a. Select the folder. b. Click ♡.

File Station adds the selected folder to the Favorites folder.

Removing a Folder from Favorites

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

Method	Steps
Using the toolbar	a. Select the folder. b. Click . c. Select **Remove from Favorites**.
Using the context menu	a. Right-click the folder. b. Select **Remove from Favorites**.
Use the Favorites button	a. Select the folder. b. Click ♡.

File Station removes the selected folder from the Favorites folder.

Compressing a Folder

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 **Compress(Zip)**.
Using the context menu	**a.** Right-click the folder. **b.** Select **Compress(Zip)**.

4. Configure the folder compression settings.

Option	Task
Archive name	Specify a name for the compressed file.
Compression level	Select the type of compression method. • Normal - Standard compression • Maximum compression - Prioritizes compression quality • Fast compression - Prioritizes compression speed
Archive format	Select the format of file compression. • zip • 7z
Update mode	Specify how the files should be updated. • Add and replace files - Add and replace the specified files. • Update and add files - Update old files and add new files. • Update existing files - Update older versions of existing files. • Synchronize files - Update old files, add new files, and remove files that are no longer in the folder.

5. Optional: Specify a password to encrypt the file.
6. Click **OK**.
   File Station compresses the selected folder and creates an archive file.

Deleting a Folder

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

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

	b. Select **Delete**.
Use the keyboard	Press **Delete**.

A confirmation message appears.

4. Specify how to delete the folder.
   - Move to Network Recycle Bin
   - Delete permanently
5. Click **OK**.
   File Station either moves the selected folder to the Recycle Bin or deletes it permanently.

Creating a Shared Folder

1. Open File Station.
2. On the menu bar, click .
3. Select **Shared Folder**.
   The **Create Shared Folder Wizard** windows opens.
4. Configure the folder settings.

Field	Description
Folder Name	Specify a folder name that contains 1 to 64 characters and that does not: • Begin or end with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : | * ? < > ; [ ] % `.
Comment (optional)	Specify a comment that contains 1 to 128 ASCII characters.
Storage Pool	Specify the storage pool where the shared folder will be created.
Space Allocation	Select one of the following space allocation options: • **Thick provisioning** • **Thin provisioning**
Allocate folder quota	You can allocate a folder quota for the snapshot shared folder.

5. Configure storage settings.

Field	Description
Data reduction	• **Compression** • **Deduplication**

Field	Description
Performance	• **SSD cache** **Note** You must create and enable SSD cache to select this option • **Fast clone**: This option allows you to copy data faster within individual shared folders and LUNs.
Synchronous I/O	• **Auto** • **All** • **None**
Performance profile (block size)	Select the block size for I/O acceleration.

6. Optional: Configure user access permissions.
   a. Under **Configure access privileges for users**, click **Edit**.
   b. Specify access permissions for each user.
7. Optional: Enable folder encryption.
   a. Under **Folder Encryption**, click **Edit**.
   b. Select **Encryption**.
   c. Specify the following information.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " $: = \
Verify Password	The password must match the previously specified password.
Save encryption key	When enabled, QuTS hero automatically unlocks the shared folder after the NAS restarts. When disabled, the administrator must unlock the folder after 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.

8. Configure WORM settings.
   a. Under **WORM Settings**, click **Edit**.

b. Select **WORM**.

c. Select one of the following options:

- **Enterprise**: You can write data to the shared folder, but you cannot modify, delete, or restore data in it. You are allowed to remove the shared folder.
- **Compliance**: You can write data to the shared folder, but you cannot modify, delete, or restore data in it. You are not allowed to remove the shared folder. To delete data in the folder, you must remove the folder's parent storage pool.

- When Write Once Read Many (WORM) is enabled, data stored in the shared folder cannot be modified or deleted.
- WORM cannot be disabled or modified after folder creation.

9. Optional: Configure advanced settings.

a. Under **Advanced Settings**, click **Edit**.

b. Configure the following settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
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 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.
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is installed on the NAS.
Enable access-based share enumeration (ABSE)	When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders.
Enable access-based enumeration (ABE)	When enabled, users can only see the files and folders that they have permission to access.

10. Click **OK**.
File Station creates a shared folder.

Sharing Space with a New User

1. Open File Station.
2. On the menu bar, click .
3. Select **Share space with a user**.
   The **Create a User** window opens.
4. Specify the following information:

Field	Description
Username	Specify a username that contains 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Special characters: ~ ! @ # $ ^ & ( ) - _ . { }
Password	Specify a password that contains 1 to 64 ASCII characters.
Quota	Specify the storage capacity available to the user.
Phone number (optional)	The information is for your reference and is not used by QuTS hero.
Email (optional)	QuTS hero sends a notification to this email address when the account password is about to expire. **Note** • You must configure the related settings in **SMTP Server** and **Change Password**. Otherwise, QuTS hero would not send notifications to the specified email address. • **SMTP Server**: Go to **Control Panel** > **System** > **Notification** > **E-mail** . • **Change Password**: Go to **Control Panel** > **System** > **Security** > **Password Policy** .
(Optional) Send a notification mail to the newly created user	When selected, QuTS hero sends a message that contains the following information to the specified email address. • Username and password • URLs for connecting to the NAS

5. Click **Create**.
   File Station creates a new user account and allocates the specified storage space.

Adding a Folder to the Transcoding Folder

Important
Video files cannot be converted to a resolution higher than the original resolution. If a higher resolution is selected, File Station automatically transcodes the file in its original resolution.

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 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. Click **OK**.

File Station adds the transcoded files to the @Transcode folder.

Canceling or Deleting Transcoding

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

Method	Steps
Using the toolbar	**a.** Select the folder. **b.** Click . **c.** Select **Cancel/Delete Transcoding**.
Using the context menu	**a.** Right-click the folder. **b.** Select **Cancel/Delete Transcoding**.

A confirmation message appears.

4. Click **OK**.
   File Station removes the selected folder from the Transcode folder and cancels the transcoding process.

Locking or Unlocking an Encrypted Shared Folder

After creating an encrypted shared folder, you can lock or unlock this folder to control user access. For details on how to create an encrypted shared folder, see Creating a Shared Folder.

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**.

Keeping a Folder or a File in Reserved Cache

You can keep the most important or the most frequently used data in the reserved cache to enhance access performance. HybridMount is required for this task.

Important
You can only perform this operation for folders in the shared folders mounted via HybridMount. For details on how to use HybridMount and how to mount cloud services, see HybridMount Help.

1. Open File Station.
2. Select a mounted shared folder.
3. Select a folder or file.
4. Choose one of the following methods.

Method	Steps
Using the toolbar	**a.** Click . **b.** Select **Always Keep in Reserved Cache**. A confirmation message appears. **c.** Click **OK**.
Using the context menu	**a.** Right-click the selected item. **b.** Select **Always Keep in Reserved Cache**. A confirmation message appears. **c.** Click **OK**.

File Station keeps the selected folder or file in the reserved cache.

Folders or files in the reserved cache can have one of the following statuses.

Status Icon	Description
	This file or folder is only stored in the cloud
	File Station is downloading this file or folder.
	File Station has encountered an error when downloading this file or folder.
	File Station has cached and is uploading this file or folder.
	File Station has cached and placed this file or folder in the upload queue.
	File Station has encountered an error when uploading this file or folder.
	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.

Removing a Folder from Reserved Cache

You can remove folders from the reserved cache.

Important
You can only perform this operation for folders in the shared folders mounted via HybridMount. For details on how to use HybridMount and how to mount cloud services, see HybridMount Help.

1. Open File Station.
2. Select a mounted shared folder.
3. Locate one or more folders.

4. Choose one of the following methods.

Method	Steps
Using the toolbar	**a.** Select one or more folders. **b.** Click . **c.** Select **Do Not Keep in Reserved Cache**. A confirmation message appears. **d.** Click **OK**.
Using the context menu	**a.** Select one or more folders. **b.** Right-click the folder. **c.** Select **Do Not Keep in Reserved Cache**. A confirmation message appears. **d.** Click **OK**.

6. Storage & Snapshots

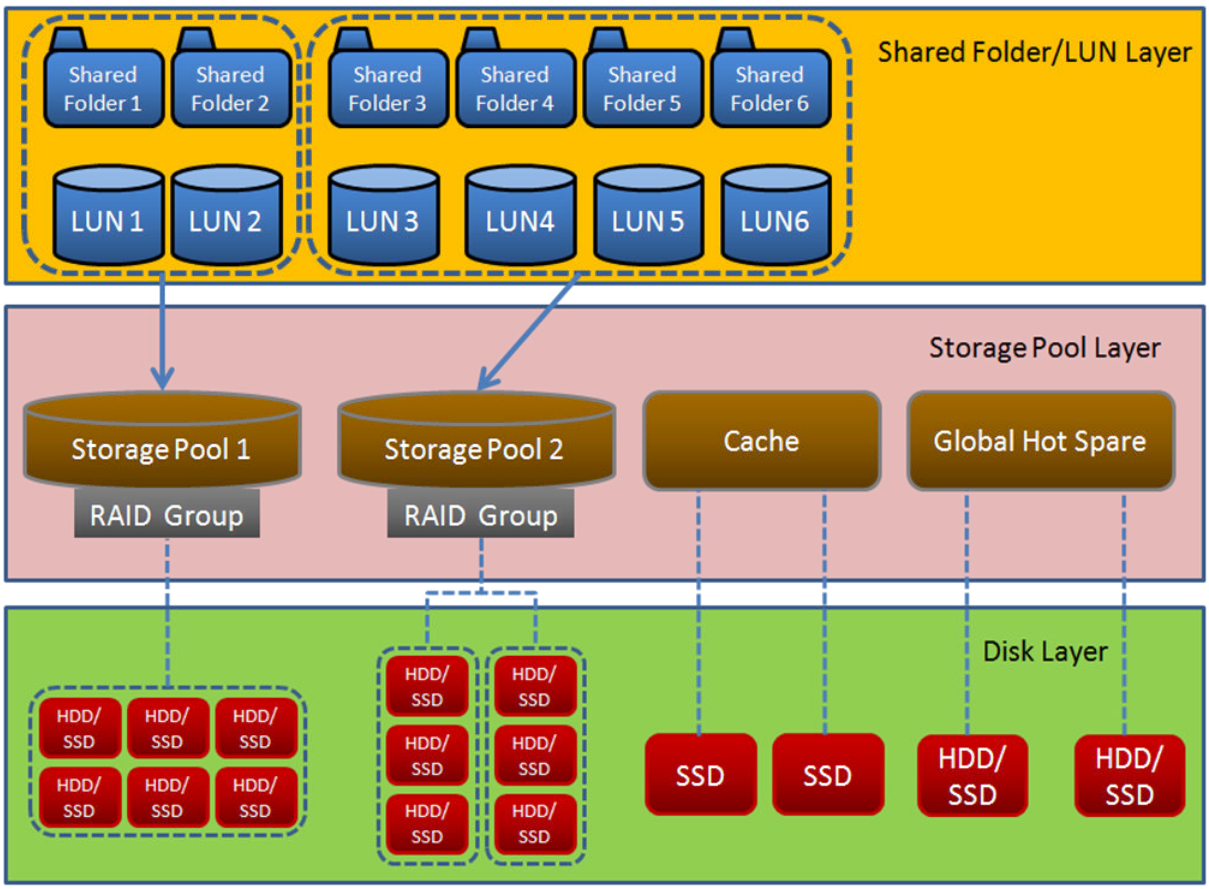
Storage & Snapshots is a QuTS hero utility that helps you create, manage, and monitor storage on your NAS. With Storage & Snapshots you can perform the following tasks:

- Create RAID groups, storage pools, and shared folders.
- Monitor storage usage and access speeds.
- Back up data using snapshots.
- Accelerate the performance of your NAS by creating an SSD cache.
- Specify which hosts (computers, servers, other NAS devices) are allowed to access the NAS.

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



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 & Snapshots window.

Storage Global Settings

Setting	Description
Pool Scrubbing Schedule	Pool scrubbing detects and automatically repairs damaged data blocks in the ZFS file system. **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.
Clean Deduplication Table	When ZFS performs deduplication, it records duplicate data in a deduplication table. Cleaning removes unused entries from the deduplication table. **Important** While the clean deduplication table task is running, the read and write performance of the system may be reduced. You should schedule this task scrubbing to run during times of low NAS usage.

Disk Health Global Settings

Setting	Description
Activate Predictive S.M.A.R.T. Migration	Enable this feature to regularly monitor disk health. If S.M.A.R.T. errors are detected on a disk, 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.

Setting	Description
TLER/ERC Timer	Enable this feature to specify a maximum response time of all disks in seconds. When a disk encounters a read or write error, it may become unresponsive while the disk firmware attempts to correct the error. 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.
Share my disk analysis data with QNAP	Enable this feature to send de-identified disk analysis data and NAS system information to QNAP to improve future products. QNAP does not collect any user data. You can opt out of this program at any time. If the app DA Drive Analyzer is installed, enabling this setting sends disk analysis data that is linked to your QID to QNAP. **Note** Disabling this setting causes the app DA Drive Analyzer to stop working.
SSD Estimated Life Warning	Enable this feature to change the disk status of an SSD to "Warning" when its estimated life is lower than the specified threshold.

Snapshot Global Settings

Setting	Description
Smart Snapshot Space Management	Enable this feature to automatically delete the oldest snapshots when the available snapshot storage space (guaranteed snapshot space plus free storage pool space) is less than 32GB. You can choose to exclude the most recent snapshot, or snapshots that were created with the setting **Keep this snapshot permanently**. When this feature is enabled and the snapshot retention policy is set to "Smart Versioning", the system will retain the latest snapshot of each time interval when deleting snapshots. For details, see Snapshot Retention Policy. **Important** • If QuTS hero is unable to create 32GB of free snapshot space, it will not create any new snapshots. • After QuTS hero has freed up more than 40GB of snapshot space, it stops deleting old snapshots.
Enable File Station Snapshot Directory for administrators	Enable this feature to consolidate all available snapshots into a centralized folder in File Station. You can restore files and folders from the snapshot directory by copying them into another folder.

Setting	Description
Make snapshot directory (@Recently-Snapshot) visible in shared folder root	Enable this feature to show a read-only folder `@Recently-Snapshot` at the root level of each shared folder, containing all of the shared folder's snapshots. You can restore files and folders from `@Recently-Snapshot` by copying them into another folder.
When the number of snapshots reaches maximum	Specify the default 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 Vault. For Snapshot Vault, you can set the maximum number of snapshots when configuring a Snapshot Replica job. For details, see Creating a Snapshot Replica Job.
Use timezone GMT+0 for all new snapshots	Enable this feature to use the GMT+0 time zone in the file names of new snapshots. This file naming convention can simplify snapshot management especially when working with snapshots from NAS devices located in different time zones. This setting only applies to new snapshots. Existing snapshots are not renamed.
Show hidden files in Snapshot Manager	Enable this feature to display hidden files in Snapshot Manager. This setting does not affect files inside the File Station Snapshot Directory.
Enable Windows Previous Versions	When enabled, Windows users can view and restore files from snapshots using the Previous Versions feature in Windows. You can disable this feature for individual folders by modifying the folder's properties.

Storage

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

Disk Type	Installation Method	SSD Cache	Storage Pools
PCIe NVMe M.2 SSD	QM2 card	Yes	Yes
PCIe NVMe M.2 SSD	Third-party M.2 to PCIe adapter card	Yes	No
SATA M.2 SSD	QM2 card	Yes	Yes
SATA M.2 SSD	NAS internal M.2 slot	Yes	Yes
PCIe form-factor SSD	PCIe slot	Yes	No

Disk Management

You can manage disks at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** . Select a disk to view its status and hardware details.

Disk Status

Status	Description
Data	The disk is being used for data storage.
Spare	The disk is configured as a hot spare.
Free	The disk is not in use.
Cache	The disk is being used in the SSD cache.
None	There is no disk in the drive bay.
Warning	QuTS hero has detected S.M.A.R.T. errors. Run a full S.M.A.R.T. test and a disk scan.
Error	QuTS hero has detected I/O errors. You must replace the disk immediately.
Safely Detached	The disk's storage pool or expansion unit was safely detached from the NAS.

Disk Information

Information	Description
Disk Health Status	The general health status of the disk • Good: The disk is healthy. • Warning: QuTS hero has detected an error. Run a full S.M.A.R.T. test and a disk scan. • Error: QuTS hero has detected a critical error. You must replace the disk immediately.
Manufacturer	The manufacturer of the disk
Model	The disk model

Information	Description
Disk Capacity	The capacity of the disk, in both binary and decimal formats **Note** • Binary format assumes that 1 GB = 1,073,741,824 bytes. This is the true capacity of the disk and is used by computers and operating systems such as QuTS hero. • Decimal format assumes that 1 GB = 1,000,000,000 bytes. This format is used by disk manufacturers and appears in advertising, on the disk's box, and in the disk's hardware specifications. • Due to differences in the number of bytes per gigabyte, a disk's binary capacity will be slightly lower than its decimal capacity. For example, a disk advertised as 500 GB (decimal) has a true capacity of 456 GB (binary).
Bus Type	The interface that the disk uses
Supported Bus Types	The disk types the drive bay supports. For example, an internal M.2 SSD slot might support SATA and NVMe SSDs.
Status	The hardware status of the disk
Current Speed	The speed at which the disk is connected to the enclosure
Maximum Speed	The maximum transfer speed supported by the drive bay or slot that the disk is installed in
Temperature	The current temperature of the disk Disk temperature is retrieved from the disk's firmware using S.M.A.R.T.
Disk Access History (I/O)	• Good: QuTS hero has not detected any I/O errors on the disk. • Error: QuTS hero has detected one or more I/O errors on the disk.
Disk SMART Information	**Important** If any of the S.M.A.R.T. attribute values reach the threshold set by the disk manufacturer or a predefined threshold determined by QuTS hero, this field will change to `Warning`.
Estimated Life Remaining	The remaining life of the disk, as calculated by the disk's firmware. When the value reaches 0, you should replace the disk. This information is only available for solid-state drives (SSDs).

Disk Actions

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

Action	Description
Scan for Bad Blocks	Scan 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** .
Locate	Prompt the drive LEDs to blink so that you can locate the drive in a NAS or expansion unit.
Detach	Remove the disk from its RAID group. The group must be of type: RAID 1, RAID 5, RAID 6, RAID 10.
Set as Enclosure Spare	Assign the disk as a global hot spare for all RAID groups within the same enclosure (NAS or expansion unit). For details, see Configuring an Enclosure Spare Disk.
Disable Spare	Unassign the disk as a global hot spare.
Secure Erase	Permanently erase all data on a disk. For details, see Secure Erase.
RAID Group	Select a RAID group to view its RAID type, capacity, and member disks.

Disk Health Information

Tab	Description	Actions
Summary	Displays an overview of S.M.A.R.T. disk information and the results from the most recent disk scan and S.M.A.R.T. test.	-
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.	Click one of the following buttons: • **Test**: Run an IHM test now. **Note** The IHM test is only available for HDDs. • **Set Schedule**: Run the IHM test periodically on a schedule. • **Statistics**: View IHM data read/write statistics.
SSD Features List	Displays all supported SSD ATA features.	-

Tab	Description	Actions
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 will change to `Warning`.	-
Test	Run a S.M.A.R.T. disk self-test.	Select one of the following options: • **Rapid Test**: Tests the electrical and mechanical properties of the disk, and a small portion of the disk surface. The test takes approximately one minute. • **Complete Test**: Tests the electrical and mechanical properties of the disk, and the full disk surface. This test duration varies depending on the storage environment.
Settings	Disk settings can be applied individually, or to multiple disks at once.	Configure the following settings: • **Enable temperature alarm**: QuTS hero displays a warning when the disk temperature is equal to or above the specified threshold. • **S.M.A.R.T. Test schedule**: Schedule periodic rapid and complete S.M.A.R.T. disk tests. The results are displayed on the **Summary** screen. • **IronWolf Health Management**: Schedule a daily IHM test for the disk. The results are saved in the selected shared folder, and are displayed on the **IronWolf Health Management** screen. **Tip** You can apply these settings to the current disk, all disks, or to disks with the same type as the current disk (HDD or SSD).

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

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

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

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

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

Testing Disk Performance on a Schedule

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
2. Click **Performance Test**.
   The **Performance Test** screen appears.
3. Set **Weekly Test** to **On**.
   A confirmation message appears.
4. Click **OK**.

QuTS hero runs a sequential read test for all disks every Monday at 6.30am, and then displays the results on the **Performance Test** screen.

Secure Erase

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

Securely Erasing a Disk

Only administrators can perform this task.

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

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
2. Select a free disk.
3. Click **Action**, and then select **Secure Erase**.

The **Secure Erase** window opens.

4. Optional: Select additional disks to erase.
5. Click **Next**.
6. Select an erase mode.

Mode	Description
Complete	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. Select **Customized** to configure the following the erase settings. • Number of rounds: QuTS hero writes over all blocks on the disk the specified number of times. • Overwrite with: Overwrite all blocks with zeros, ones, or a random zero or one.
SSD	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.
Fast	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.

7. Click **Next**.
8. Enter your password.

Note
You must be logged in as an administrator.

9. Click **Apply**.

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

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.

Creating a Storage Pool

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

NAS State	Action
No storage pools	Click **New Storage Pool**.
One or more storage pools	Click **Create**, and then select **New Storage Pool**.

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

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

Important

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

5. Select one or more disks.

Important

- QuTS hero assigns the first storage pool created as the system pool. The system pool should consist of only SSDs.
- If you select RAID 5, 6, TP, 10, 50, or 60 for the RAID type in the next step, you cannot select more than 16 disks.

For details, see The System Pool.

Warning
All data on the selected disks will be deleted.

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. 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.

8. Optional: Enable 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.

Note

- QSAL is available for the following RAID types: RAID 5, 6, 50, 60, TP.
- QSAL can only be enabled when creating a new pool and cannot be disabled later.

9. Click **Next**.
10. Configure any of the following settings.

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 storage pool space. • Optimizing the pool will take a long time. While the pool is being optimized, the pool will be unavailable and you cannot create another pool with Optimize Performance enabled.
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.

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.
Enable 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 is equal to or above the specified threshold.

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

QuTS hero creates the storage pool and then displays the information on the **Storage/Snapshots** screen.

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 pools 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.

Storage Pool Management

Deleting a Storage Pool

Only administrators can perform this task.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
4. Click **Remove**, and then select **Remove Pool**.
   A notification window opens.
5. Select **Remove every shared folder, LUN, and snapshot vault in this storage pool**.

Warning
All data in the storage pool will be deleted.

6. Click **OK**.
   The **Remove Pool** window opens.
7. Enter your password.

Note
You must be logged in as an administrator.

8. Click **OK**.

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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Pool Scrubbing**.
   The **Start Storage Pool Scrub** window opens.
5. Click **OK**.

Configuring a Storage Pool Space Alert

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Set Threshold**.
   The **Alert Threshold** window opens.
5. Enable space alerts.
6. Specify an alert threshold.
   QuTS hero issues a warning notification when the percentage of used space is greater than or equal to the specified threshold.
7. Click **Apply**.

Storage Pool Status

Status	Description
Ready	The storage pool is working normally. All RAID groups in the pool have the status `Ready`.

Status	Description
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 (Rebuilding)	One or more RAID groups in the storage pool have the status `Degraded (Rebuilding)`. QuTS hero is currently rebuilding them due to disk failure.
Warning (Read-Only)	One or more RAID groups in the storage pool have the status `Not Active`. **Note** It might be possible to recover some data from shared folders and LUNs.

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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Configure Over-Provisioning**.
   The **Configure Over-Provisioning** window opens.
5. Enable over-provisioning.
6. Set the percentage of storage pool space to reserve for over-provisioning.

Tip
The default value is 5%.

7. 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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Actions**.
5. Under **Resync Priority**, select one of the following priorities.

- **Service First**: QuTS hero performs RAID operations at lower speeds in order to maintain NAS storage performance.
- **Default**: QuTS hero performs RAID operations at the default speed.
- **Resync First**: QuTS hero performs RAID operations at higher speeds. Users may notice a decrease in NAS storage performance while RAID operations are in progress.

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

Important

- You cannot select disks from multiple expansion units.

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

8. Select one or more disks.

Warning
All data on the selected disks will be deleted.

9. Click **Next**.
10. Review the summary information.
11. Click **Expand**.
    A confirmation message appears.
12. 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 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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Select a RAID group.
   The RAID group can be of any type except for RAID 0.
5. Ensure there are no global spare disks assigned to the RAID group's enclosure.
   You can view and disable global enclosure spare disks at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
6. Prepare a number of higher-capacity disks.
   You must prepare one higher-capacity disk for each disk in the RAID group.
7. Click **Manage**, and then select **Replace Disks One by One**.
   The **Replace Disks One by One** window opens.
8. Select a disk to replace.
9. Click **Change**.
   The disk description changes to `Please remove this drive`.
10. Remove the disk from the drive bay.
    - The NAS beeps twice.
    - The disk description changes to `Please insert the new disk`.
    - The status of the RAID group changes to `Degraded`.

- The status of the RAID group's storage pool changes to `Warning(Degraded)`.

11. 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`.
12. 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`.
13. Repeat the previous steps 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 QuTS hero, or both be running QTS. QuTS hero to QTS migration is not possible.
- The version of QuTS hero or QTS running on the new NAS must be the same or newer than the version running on the original NAS.

Migrating a Storage Pool to a New NAS

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Click **Action**, and then select **Safely Detach Pool**.
   A confirmation message appears.
5. Click **Yes**.
   The storage pool status changes to `Safely Detaching...`. After QuTS hero has finished detaching the pool, it disappears from Storage & Snapshots.
6. Remove the drives containing the storage pool from the NAS.
7. Install the drives in the new NAS.

8. On the new NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
9. Click **Recover**, and then select **Attach and Recover Storage Pool**.
   A confirmation message appears.
10. Optional: Enter the SED password.
    You must enter this password if you were using self-encrypted drives (SEDs) with encryption enabled.
11. Click **OK**.
    QuTS hero scans the disks and detects the storage pool.
12. Click **Apply**.

The storage pool appears in Storage & Snapshots on the new NAS.

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 & Snapshots** > **Storage** > **Storage/Snapshots** .
- A QuTS hero shared folder is the same as a QTS volume that contains one shared folder.

Creating a Shared Folder

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Click **Create**, and then select **New Shared Folder**.
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 first characters cannot be a space.
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, guaranteeing that space will be 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 the 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	Amount of free space in the parent storage pool.
Thin provisioning	1 PB **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.

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.
9. Optional: Enable folder encryption.
   a. Under **Folder Encryption**, click **Edit**.
   b. Select **Encryption**.
      Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.
   c. Specify the following information.

Field/Option	Description
Input Password	Specify a password that contains 8 to 32 characters except the following: " $: = \ This field does not support multibyte characters.
Verify Password	The password must match the previously specified password.
Save encryption key	When enabled, QuTS hero automatically unlocks the shared folder after the NAS restarts. When disabled, the administrator must unlock the folder after the NAS restarts. For details, see Unlocking a Shared Folder. **Warning** • Saving the encryption key on the NAS can result in unauthorized data access if unauthorized personnel are able to physically access the NAS. • If you forget the encryption password, all data will become inaccessible.

10. Click **Next**.

11. Optional: Configure any of the following storage 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 filesystems. 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 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
Synchronous I/O	Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes: • Standard: 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	Specify how the shared folder will be used. Each option results in a different record size, optimizing performance for the specified application. **Tip** The default is 64K.

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. Select **WORM**.

b. Configure any of the following settings.

Setting	Description
WORM type	Select a WORM type. • 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.

Setting	Description
Lock delay	When enabled, a file added to the folder can be modified within the lock delay time period. After this time has passed, the file automatically becomes locked and unmodifiable. **Note** • The maximum lock delay is 168 hours and 59 minutes. • You cannot modify lock delay after folder creation. • The time a file becomes locked might vary from the specified time by +/- 1 minute.
Retention	Limit how long WORM applies to each file and folder. Files and folders can be modified after the specified time period.

13. Click **Next**.
14. Optional: Configure user access permissions.
    a. Under **Configure access privileges for users**, click **Edit**.
    b. Specify the access permissions for users.
    For details, see Shared Folder Permissions.
15. Click **Next**.
16. Optional: Configure advanced settings.

Option	Description
Guest Access Right	Select the permission level assigned to users without a NAS account.
Hide network drive	Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
SMB Encryption	This option is available only when SMB3 is enabled and 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.
Restrict the access of Recycle Bin to administrators only for now	Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. **Note** This option is available only when **Enable Network Recycle Bin** is selected.
Enable sync on this shared folder	Selecting this option allows this shared folder to be used with Qsync. This option is only available if Qsync Central is installed on the NAS.

Option	Description
Enable access-based share enumeration (ABSE)	When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders.
Enable access-based enumeration (ABE)	When enabled, users can only see the files and folders that they have permission to access.
Set this folder as the Time Machine backup folder (macOS)	When enabled, the shared folder becomes the destination folder for Time Machine in macOS.

17. Click **Next**.
18. Review the summary information, and then click **Finish**.

Shared Folder Management

To open this screen, go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** , select a shared folder, and then click **Manage**.

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 filesystems. 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 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
Synchronous I/O	Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes: • All: 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. • Auto: QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • 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.
Remove	Delete the shared folder. For details, see Deleting a Shared Folder.
Resize Shared Folder	Change the storage capacity of a shared folder. For details, see: • Expanding a Shared Folder • Shrinking a Shared Folder
Actions	Configure the settings of the shared folder. For details, see Shared Folder Actions.
View data reduction information	View statistics related to compression and deduplication. For details, see Data Reduction.

Shared Folder Actions

Action	Description
Edit WORM Settings	Edit the WORM retention time of the folder. **Note** WORM must be enabled on the folder and set to `Enterprise`.
Edit Properties	Configure the shared folder's storage settings.
Edit Permission	Configure user access permissions.
Statistics	View data reduction statistics for the shared folder.
Set threshold	Configure a space alert for the shared folder. For details, see Configuring a Shared Folder Space Alert.

Action	Description
Rename Shared Folder	Change the name of the shared folder. • 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 first characters cannot be a space.
Convert to Thick	Change the space allocation method from thin provisioning to thick provisioning.
Convert to Thin	Change the space allocation method from thick provisioning to thin provisioning.

Deleting a Shared Folder

Note
If an application such as SnapSync is using the shared folder, then you need to stop the application from using the folder before deleting it.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.
3. Click **Manage**.
   The **Shared Folder Management** window opens.
4. Click **Remove**.
   A confirmation message appears.

Warning
All data in the shared folder will be deleted.

5. Click **Apply**.

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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.
3. Click **Manage**.
4. Click **Resize Shared Folder**.

The **Shared Folder Resizing Wizard** opens.

5. Specify a new larger capacity for the shared folder.
   Capacity can be specified in megabytes (MB), gigabytes (GB) or terabytes (TB).

Method	Maximum Size
Thick provisioning	Amount of free space in the parent storage pool.
Thin provisioning	1 PB **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.

6. Optional: Click **Set to Max**.
   Sets the new shared folder capacity to the maximum available size. This option is only available for thick shared folders.
7. 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 & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.
3. Click **Manage**.
4. Click **Resize Shared Folder**.
   The **Shared Folder Resizing Wizard** opens.
5. Specify a new smaller capacity for the shared folder.
   Capacity can be specified in megabytes (MB), gigabytes (GB) or terabytes (TB).
6. Click **Apply**.
   A confirmation message appears.
7. Click **OK**.
   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`.

Configuring a Shared Folder Space Alert

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.
3. Click **Manage**.
   The **Shared Folder Management** window opens.
4. Click **Actions**, and then select **Set Threshold**.
   The **Alert Threshold** window opens.
5. Enable space alerts.
6. Specify an alert threshold.
   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:

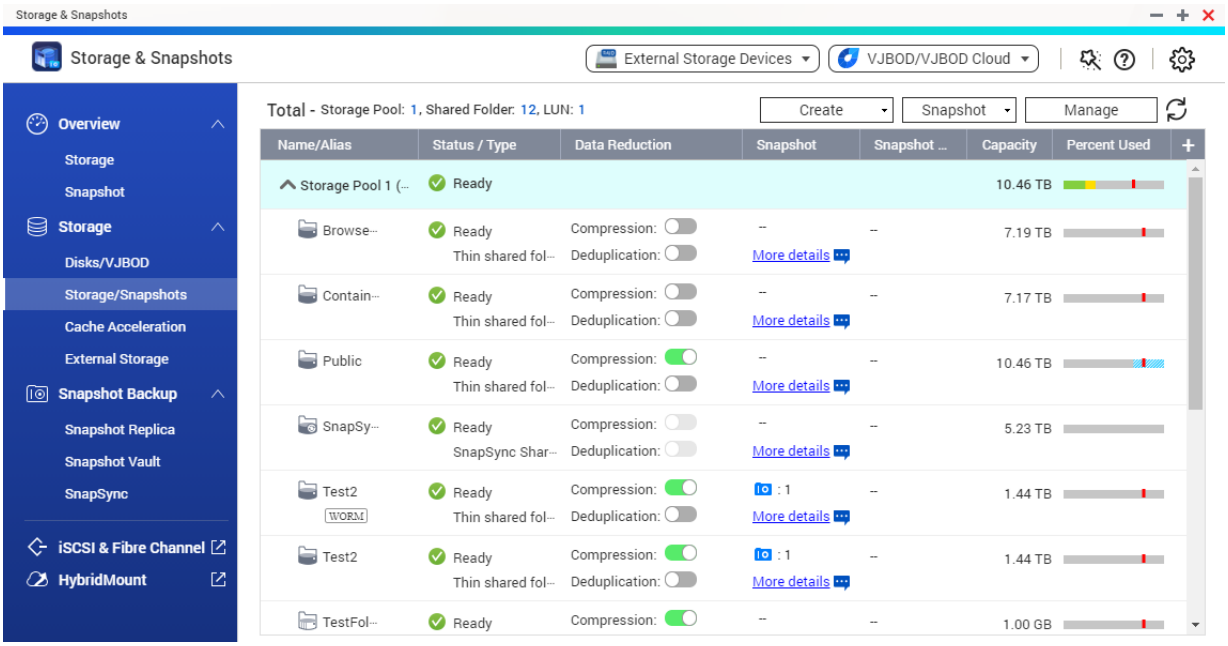
Feature	Description
Compression	Compression attempts to reduce the size of stored files by removing redundant data within each file. Making files smaller means less storage space is consumed and more files can be stored on the NAS.
Deduplication	Deduplication is a technique for eliminating duplicate 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 8 GB of memory.

Configuring Compression and Deduplication

To quickly enable or disable compression or deduplication, go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** and then use the toggle buttons in the **Data Reduction** column.

Important

- Disabling compression only affects new data. Existing data in the folder remains compressed.
- Disabling deduplication only affects new data. Existing data in the folder remains deduplicated.



Viewing Data Reduction Statistics

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
   The **Storage Pool Management** window opens.
4. Go to the **Data Reduction** tab.

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.

RAID Feature	Description	Advantages	Disadvantages
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 and capacity when creating a RAID group.
- Increasing the number of disks in a RAID group increases the risk of simultaneous disk failure and lengthens rebuild times. 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	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	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	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 (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	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 60	≥ 8	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.

RAID Type	Number of Disks	Disk Failure Tolerance	Overview
Triple Mirror	3	2	• An identical copy of data is stored on three disks. • There is also 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	3	• Data and parity information are striped across all disks. • The capacity of three disks are lost to store parity information. • RAID-TP adds an extra level of redundancy over RAID 6.

RAID Actions

Tip
To perform any of the following actions:

1. Go to **Storage & Snapshots** > **Overview** > **Storage** .
2. Select a storage pool.
3. Click **Manage**.
4. Select a RAID group.
5. Click **Manage**.

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.
Recover	Recovers the RAID group from accidental disk removal. For details, see Recovering a RAID Group.

RAID Group Status

Status	Description
Ready	The RAID group is working normally.

Status	Description
Degraded	One or more disks in the RAID group have failed. The number of disk failures are within the disk failure tolerance of the RAID group. There are not enough spare disks available to QuTS hero to replace all the failed disks.
Degraded (Rebuilding)	One or more disks in the RAID group have failed. The number of disk failures are within the disk failure tolerance of the RAID group. QuTS hero has replaced the failed disks with spare disks, and is now rebuilding the RAID group.
Not active	One or more disks in the RAID group have failed. The number of disk failures exceeds the disk failure tolerance of the RAID group.

RAID Disk Failure Protection

All RAID types except for RAID 0 can tolerate a specific number of disk failures without losing data. When a disk in a RAID group fails, the RAID group status changes to `degraded` and then 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 `Ready` after rebuilding has finished.
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 space disk acts as a hot spare for all RAID groups within a single enclosure (NAS or expansion unit). Under normal conditions, the enclosure space disk is unused and does not store any data. When a disk in any RAID group fails, the hot spare disk automatically replaces the faulty disk.

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

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

Warning
All data on the selected disk will be deleted.

4. Click **Action**, and then select **Set as Enclosure Spare**.
   A confirmation message appears.
5. Click **OK**.

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

Recovering a RAID Group

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

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

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

1. Reconnect all disconnected disks.

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

2. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
3. Select a storage pool with the status `Inactive`.
4. Click **Manage**.
   The **Storage Pool Management** window opens.
5. Select a RAID group with the status `Error`.
6. Click **Manage**, and then select **Recover RAID**.

QuTS hero starts to rebuild the RAID group.

Self-Encrypting Drives (SEDs)

A self-encrypting drive (SED) is a drive with encryption hardware built into the drive controller. An SED automatically encrypts all data as it is written to the drive and decrypts all data as it is read from the drive. Data stored on an SED is always fully encrypted by a data encryption key (DEK). The DEK can also be encrypted by a user-specified authentication key (AK) that allows the SED to be locked and unlocked. Both encryption keys are stored in the drive's hardware and cannot be accessed by the host operating system or unauthorized users.

Creating an SED Secure Storage Pool

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

NAS State	Action
No storage pools	Click **New Storage Pool**.
One or more storage pools	Click **Create**, and then select **New Storage Pool**.

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

3. Click **Next**.

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

Important

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

5. Select **Create SED secure storage pool**.
The list of disks only displays SED disks.
6. Select one or more disks.

Warning
All data on the selected disks will be deleted.

7. 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.

8. 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.

9. Click **Next**.
10. Optional: Configure 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.
11. Optional: Configure the alert threshold.
QuTS hero issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
12. Specify the SED password.
The SED 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.

13. Optional: Save the encryption key to the local NAS
    Saving the encryption key enables QuTS hero to automatically unlock and mount the SED pool when the NAS starts up. If the encryption key is not saved, you must specify the encryption password every time the NAS restarts.

Warning
Saving the encryption key can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.

14. Click **Next**.
15. Click **Create**.
    A confirmation message appears.
16. Click **OK**.

QuTS hero creates the storage pool and then displays the information on the **Storage/Snapshots** screen.

SED Storage Pool Actions

Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** , select a SED pool, click **Manage**, then select **Actions** > **SED Settings** to perform the following actions.

Action	Description
Change SED Pool Password	Change the SED security password. You can also choose to save the encryption key to the local NAS. **Warning** Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable. Saving the encryption key enables QuTS hero to automatically unlock and mount the SED pool when the NAS starts up. If the encryption key is not saved, you must specify the encryption password every time the NAS restarts. **Warning** Saving the encryption key can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.
Lock	Lock the pool. All shared folders, LUNs, snapshots, and data will become inaccessible until it is unlocked.
Unlock	Unlock a locked SED pool. All shared folders, LUNs, snapshots, and data will become accessible.
Disable SED Security	Remove user password and disable the ability to lock and unlock the pool.
Enable SED Security	Add user password and enable the ability to lock and unlock the pool.

Removing a Locked SED Storage Pool

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a locked SED storage pool.
3. Click **Manage**, and then select **Remove**.
   The **Removal Wizard** window opens.
4. Select a removal option.

Option	Description
Enter the password of the pool	QuTS hero unlocks the SED disks in the storage pool, and then deletes all data.
Forget password	QuTS hero 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 **Disks/VJBOD**, click **Recover**, and then select **Attach and Recover Storage Pool**. • Erase the disks using SED erase.

5. Click **Apply**.

SED Erase

SED Erase erases all of the data on a locked or unlocked SED disk and removes the SED security password.

Erasing a Disk Using SED Erase

1. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
2. Select an SED disk.
3. Click **Actions**, and then select **SED Erase**.
   The **SED Erase** window opens.
4. Enter the disk's PSID.

Tip
The PSID can usually be found on the front of the disk.

5. Click **Apply**.

Expansion Units

Expansion units are designed to expand the storage capacity of a QNAP NAS by adding extra drive bays. Expansion units can be connected to the NAS using USB, Mini-SAS, Thunderbolt, or other cable type.

Tip
Expansion units used to be known as JBODs.

Expansion Unit Actions

Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** and select an expansion unit to perform one of the following actions.

Action	Description
Enclosure Info	View full hardware details of the expansion unit, including the model, serial number, firmware version, BUS type, CPU temperature, system temperature, power status, and fan speeds.
Action > **Locate**	Prompt the expansion unit chassis LEDs to blink, so that you can locate the device in a server room or rack.
Action > **Safely Detach**	Stop all activity and safely unmount the enclosure from the host NAS.
Action > **Update Firmware**	Update the expansion unit's firmware.
Action > **Rename Enclosure**	Rename the selected expansion unit.
RAID Group	View details about each RAID group on the expansion unit, including its RAID type, capacity, and member disks.

Expansion Unit Automatic Recovery

If an expansion unit is accidentally disconnected from the NAS, for example by an unscheduled shutdown or disconnected cable, then the following changes to storage state will occur:

- The status of all storage pools on the expansion unit will change to `Error`.
- The status of all RAID groups on the expansion unit will change to `Not Active`.

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

Expansion Unit Recovery Actions

Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** , select an expansion unit, and then click **Recover** to perform one of the following actions.

Action	Description
Reinitialize enclosure ID	Reset all expansion unit IDs, and then give each unit a new ID number starting from 1 based on the order than 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 4.5.0 or later
External Storage	Use the RAID enclosure as an external USB disk. This mode supports multiple RAID groups. Each RAID group appears as a separate disk when the enclosure is connected to a host.	• Individual • JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10	• Windows • macOS • Linux • QNAP NAS • Other NAS devices

Storage Configuration

Creating a Storage Pool on a RAID Enclosure

Important

- The Mode switch on the RAID enclosure must be set to Software Control mode. For details, see the enclosure's hardware user guide.
- The RAID enclosure must not contain any existing RAID groups.

Warning
To prevent errors or data loss, do not change the enclosure Mode switch from Software Control to any other mode while the enclosure is connected to the NAS.

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices**, and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Configure**.
   The **External RAID Device Configuration Wizard** opens.
4. Click **Next**.
5. Select two or more disks.

Warning

- All data on the selected disks will be deleted.
- All unselected disks will be automatically assigned as spare disks, and cannot be used until the RAID group has been deleted.

6. Select a RAID type.
   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 is equal to or above the specified threshold.
13. Click **Next**.
14. Click **Create**.
    A confirmation message appears.
15. Click **OK**.

QuTS hero creates the storage pool and then displays the information on the **Storage/Snapshots** screen.

Creating a Storage Pool on a Drive Adapter

1. Set the drive adapter to the RAID mode that you want using the device's hardware Mode switch.
2. Install the drive adapter in the NAS.
   For details, see the drive adapter's hardware user guide.
3. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
4. Perform one of the following actions.
   - Click **New Storage Pool**.
   - Click **Create**, and then select **New Storage Pool**.

   The **Create Storage Pool Wizard** window opens.
5. Click **Next**.
6. Under **Enclosure Unit**, select **NAS Host**.
7. In the list of disks, select the drive adapter.
8. Under **RAID Type**, select **Single**.
9. Click **Next**.
10. Optional: Configure storage pool over-provisioning.
    Over-provisioning reserves a specified percentage of space in a storage pool in order to maintain consistent pool access performance. You can decrease the amount of space reserved for over-provisioning after QuTS hero has created the storage pool.

> **Tip**
> To determine the optimal amount of over-provisioning for your storage pool, download and run ZFS Pool Profiling Tool from App Center.

11. Optional: Configure the alert threshold.
    QuTS hero issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
12. Click **Next**.
13. Review the summary information.

14. Click **Create**.
    A confirmation message appears.
15. Click **OK**.

QuTS hero creates the storage pool and then displays the information on the **Storage/Snapshots** screen.

Configuring a RAID Enclosure as an External Storage Device

Important

- The Mode switch on the RAID enclosure must be set to Software Control mode. For details, see the enclosure's hardware user guide.
- The RAID enclosure must not contain any existing RAID groups.

Warning
To prevent errors or data loss, do not change the enclosure Mode switch from Software Control to any other mode while the enclosure is connected to the NAS.

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices**, and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Configure**.
   The **External RAID Device Configuration Wizard** opens.
4. Click **Next**.
5. Select two or more disks.

Warning

- All data on the selected disks will be deleted.
- All unselected disks will be automatically assigned as spare disks, and cannot be used until the RAID group has been deleted.

6. Select a RAID type.
   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 & Snapshots** > **Storage** > **External Storage** .
12. Select the uninitialized partition on the RAID enclosure.

> **Tip**
> Double-click on the RAID enclosure to see all of its partitions.

13. Click **Actions**, and then select **Format**.
    The **Format Partition** window opens.
14. Select a file system.

File System	Recommended Operating Systems and Devices
NTFS	Windows
HTS+	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** • Using exFAT on QuTS hero requires an exFAT driver license. You can purchase the license in License Center. • 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 volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.

Warning

- Saving the encryption key on the NAS can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.
- If you forget the encryption password, the volume will become inaccessible and all data will be lost.

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 at **Storage & Snapshots** > **Storage** > **External Storage** .

QuTS hero External RAID Management

Open **Storage & Snapshots**, click **External Storage Devices**, and then select **External Storage Device Management** to view, manage, and configure RAID devices connected to the NAS.

Warning
To prevent errors or data loss, do not change a RAID device's Mode switch from Software Control to any other mode while the device is connected to the NAS.

UI Element	Description
External storage device	Select a RAID device to manage.
Safely Detach	Disconnect a RAID device from the NAS when the device is in NAS Storage mode. QuTS hero will stop and then safely remove all storage pools, shared folders, volumes, and LUNs stored on the device, without deleting any data. You can then connect it to another NAS or computer. **Tip** To access the storage pools, shared folders, volumes, and LUNs on another QNAP NAS, connect the RAID device to the target NAS, go to **Storage & Snapshots** > **Disks/ VJBOD** then select **Recover** > **Scan all Free Disks** . **Important** This button only appears when the device is in NAS Storage mode.

UI Element	Description
Eject	Safely disconnect a RAID device from the NAS when the device is in External Storage mode. You can then connect it to another NAS or computer. **Important** This button only appears when the device is in External Storage mode.
Configure	Create a RAID group on the RAID device and configure the storage mode. **Important** The RAID device's Mode switch must be set to Software Control mode.
Check for Update	Update the RAID device's firmware, either over the internet or from a local file. For details, see Manually Updating External RAID Device Firmware in QuTS hero.
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 will automatically replace the faulty disk. For details, see Configuring a Spare Disk.
Manage > **Remove**	Delete the RAID group. The member disks will be 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/VJBOD** 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 & Snapshots** > **Storage** > **Disks/VJBOD** .
2. Select an enclosure.
3. Select **Action** > **Safely Detach** .
   The **Safely Detaching Enclosure** window opens.
4. Click **Apply**.

Warning
Do not disconnect or power off the RAID enclosure until the enclosure has been detached.

A confirmation message appears.

5. Disconnect the RAID enclosure from the NAS.
6. Connect the RAID enclosure to the target QNAP NAS.
7. On the target NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
8. Click **Recover**, and then select **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 & Snapshots** > **Storage** > **Storage/Snapshots** .

Manually Updating External RAID Device Firmware in QuTS hero

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices** and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Select a RAID device.
4. Click **Check for Update**.
   The **Firmware Management** window opens. 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 then power on the device, or disconnect 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. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
10. Click **Recover**, and then select **Attach and Recover Storage Pool**.

Configuring a Spare Disk

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices** and then select **External Storage Device Management**.
   The **External Storage Device Management** window opens.
3. Click **Manage**, and then select **Configure Spare Disk**.
   The **Configure Spare Disk** window opens.
4. Select one or more free disks.
5. Click **Apply**.

The selected disks are assigned as spare disks for the RAID group on the external RAID device.

External RAID Device Health

RAID Enclosure Health

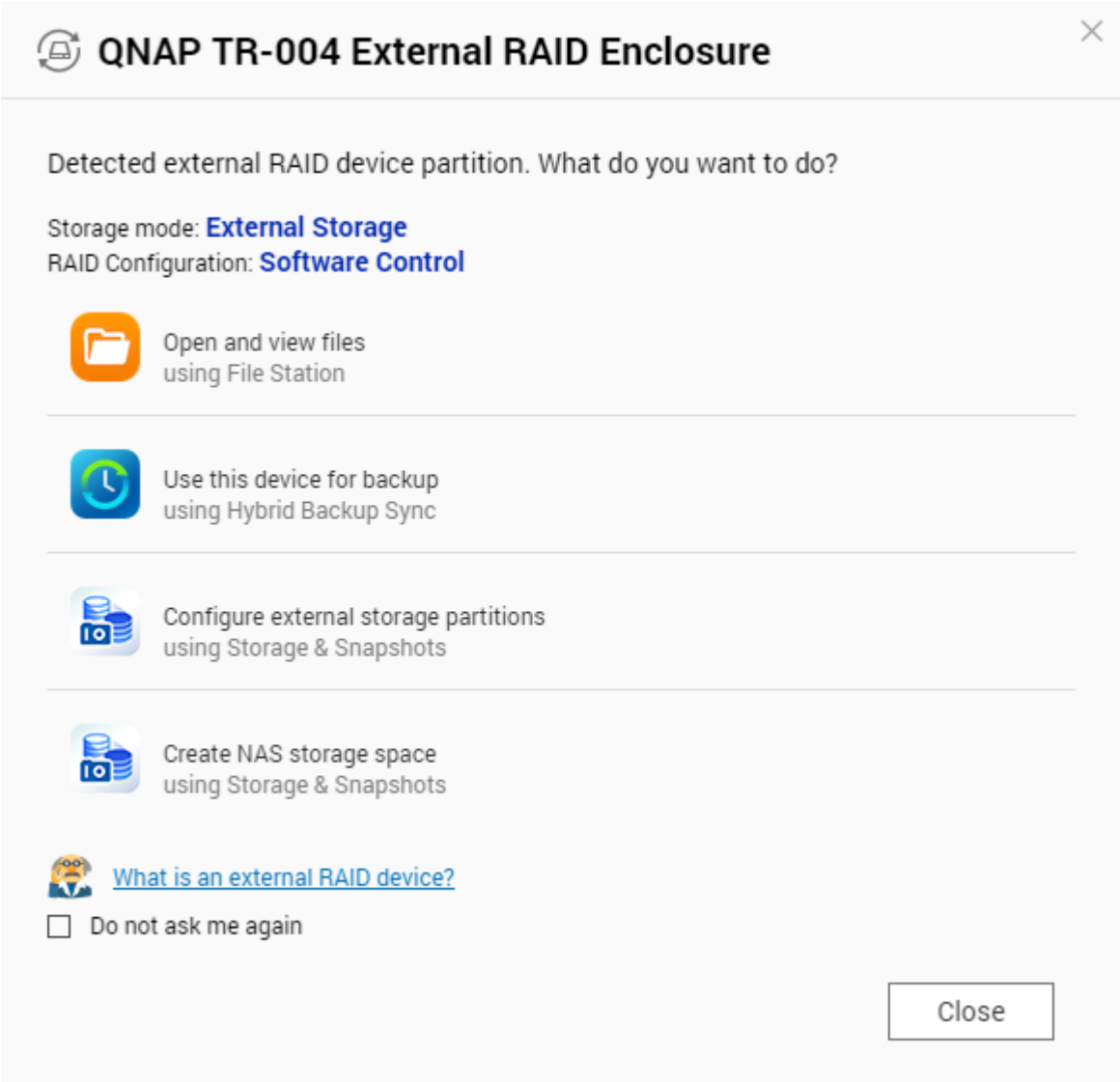
To view the status and heath of RAID enclosures connected to the NAS, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .

Drive Adapter Health

To view the status and heath of drive adapters and the disks installed in it, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .

The Autoplay Menu

The Autoplay menu opens when you connect a RAID enclosure to a NAS. The actions available in this menu vary depending on the enclosure's current storage mode and RAID configuration.



Action	Description
Open and view files	Opens the enclosure in **File Station**.
Use this device for backup	Opens **HBS**.
Configure external storage partitions	Opens **Storage & Snapshots** > **Storage** > **External Storage** . For more information, see Configuring a RAID Enclosure as an External Storage Device.
Create NAS storage space	Opens **Storage & Snapshots** > **Storage** > **Storage/Snapshots** . For more information, see: • Creating a Storage Pool on a RAID Enclosure
Edit access permissions	Opens the **Edit Shared Folder Permissions** window to edit access permissions for this device.

QNAP JBOD Enclosures

QNAP JBOD Enclosure Types

Enclosure Type	Description	Supported Platforms	Example Models
SAS JBOD enclosure	A JBOD enclosure that uses SFF interface ports to connect to a NAS. These enclosures can only be connected to a host device that has a PCIe SAS storage expansion card installed.	NAS: • QuTS hero • QTS	• TL-R1220Sep-RP, TL-R1620Sep-RP
SATA JBOD enclosure	A JBOD enclosure that uses SFF interface ports to connect to a NAS or computer. These enclosures can only be connected to a host device that has a QNAP QXP host bus adapter installed.	Computer: • Windows • Linux NAS: • QuTS hero • QTS	• TL-D400S, TL-D800S, TL-D1600S • TL-R400S, TL-R1200S-RP
USB JBOD enclosure	A JBOD enclosure that uses USB 3.2 Gen 2 Type-C ports to connect to a NAS or computer.	Computer: • Windows • Linux • macOS NAS: • QuTS hero • QTS	• TL-D800C • TL-R1200C-RP

QuTS hero JBOD Management

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

Location	Description
Disks/VJBOD	View, manage, and configure storage for attached JBOD enclosures. You can create storage pools, volumes, and RAID groups using disks installed in the JBOD enclosure.
External Storage	View and manage attached JBOD enclosures and installed disks.

Updating JBOD Enclosure Firmware in QuTS hero

1. Open **Storage & Snapshots**.
   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 then power on the device, or disconnect 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. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
5. Click **Recover**, and then select **Attach and Recover Storage Pool**.

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 Creation

Taking a Snapshot

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder or LUN.
3. Click **Snapshot** and then select **Take a Snapshot**.
   The **Take a Snapshot** window opens.
4. Optional: Specify a name.
5. Optional: Choose to keep the snapshot permanently.
   If selected, QuTS hero retains the snapshot indefinitely. If not selected, QuTS hero may delete the snapshot according to the snapshot retention policy set for the shared folder or LUN.
6. Select the LUN snapshot type.
   This setting is only available when taking a snapshot of a block-based LUN.

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

Type	Description
Application consistent	The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QuTS hero takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot. **Important** This option is only available for VMware vCenter, or for Volume Shadow Copy Service (VSS) aware applications running on a Windows server. You must install QNAP Snapshot Agent on the iSCSI initiator.

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

QuTS hero takes the snapshot. The snapshot appears in **Snapshot Manager**.

Configuring a Snapshot Schedule

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder or LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Click **Schedule Snapshot**.
   The **Snapshot Settings** window opens.
5. Select **Enable schedule**.
6. Specify how often QuTS hero will take a snapshot.
7. Select the LUN snapshot type.
   This setting is only available when taking a snapshot of a block-based LUN.

Type	Description
Crash consistent	The snapshot records the state of the data on the LUN.
Application consistent	The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QuTS hero takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot. **Important** This option is only available for VMware vCenter, or for Volume Shadow Copy Service (VSS) aware applications running on a Windows server. You must install QNAP Snapshot Agent on the iSCSI initiator.

8. Optional: Enable smart snapshots.
   When enabled, QuTS hero only takes a snapshot if data on the shared folder or LUN was modified since the last snapshot was taken.
9. Optional: Specify a description.
   The description helps you to identify the snapshot.
10. Click **OK**.
    A confirmation message appears.
11. Click **OK**.

QuTS hero starts taking snapshots according to the schedule.

Snapshot Management

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.

Configuring a 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, for example changing from `Keep for: 5 days` to `Keep for: 2 days`, then QuTS hero deletes existing snapshots to conform with the new policy.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder or LUN.
3. Click **Snapshot** and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Click **Schedule Snapshot**.
   The **Snapshot Settings** window opens.
5. Click **Snapshot Retention**.
6. Select a snapshot retention policy.

Snapshot Retention Policy	UI Label	Description
Time-based	Keep for	Keep each snapshot for the specified length of time.
Fixed number	Keep the specified number of snapshots	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	UI Label	Description
Smart versioning	Smart versioning	Keep a snapshot created during a time period for a specified length of time. Examples: • **Hourly**: 24 - At the end of every hour, the earliest snapshot created that hour becomes the hourly backup. The snapshot is retained for 24 hours and then deleted. • **Daily**: 14 - At the end of every day, the earliest snapshot created that day becomes the daily snapshot. The snapshot is retained for 14 days and then deleted. • **Weekly**: 5 - At the end of every week, the earliest snapshot created that week becomes the weekly snapshot. The snapshot is retained for 5 weeks and then deleted. • **Monthly**: 11 - At the end of every month, the earliest snapshot created that month becomes the monthly snapshot. The snapshot is retained for 11 months and then deleted. **Important** The maximum number of snapshots for all time periods combined is 256.

7. Click **OK**.

Configuring Pool Guaranteed Snapshot Space

Pool guaranteed snapshot space is storage pool space that is reserved for storing snapshots. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots.

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder or LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
4. Click **Pool Guaranteed Snapshot Space**, and then select **Configure**.
5. Enable **Enable Pool Guaranteed Snapshot Space**.

6. Select the amount of reserved space.

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

7. Click **OK**.

Deleting Snapshots

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder or LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Optional: Change the view to list view.
   a. Click .
   b. Select **List View**.
5. Select one or more snapshots.
6. Click .

Snapshot Data Recovery

Restoring Files and Folders from a Snapshot

Tip

- Use snapshot revert to quickly restore all data on a shared folder or LUN.
- You can restore files and folders from a snapshots in File Station by enabling **Enable File Station Snapshot Directory for administrators**.

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.
   The shared folder must contain at least one snapshot.
3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Select the files and folders to be restored.
6. Perform one of the following actions.

Action	Description
Select **Restore** > **Restore Files**	Restore the files or folders to their original storage location. If the files or folders still exists on the NAS, then they will be overwritten with the older versions. **Warning** All changes made after the snapshot was taken will be deleted.
Select **Restore** > **Restore Files to**	Choose one of the following restoration options. • Restore the files or folders to a different location on the NAS. • Restore the files or folders to remote mounted storage space. • Restore a single shared folder as a new shared folder.
In the menu bar, click	Download the files and folders to your computer in a ZIP file.

QuTS hero restores the files and folders then displays a confirmation message.

Reverting a Shared Folder

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.

Important
The shared folder must be the source folder for a Snapshot Replica job.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Revert Folder Snapshot**.

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

6. Click **Local Revert**.

The status of the shared folder changes to `Reverting`. QuTS hero disables access to the shared folder until the revert process is finished.

Reverting a LUN

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

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

Important
The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Revert LUN Snapshot**.

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

6. Optional: Configure the following settings.

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

7. Click **Local Revert**.

QuTS hero unmaps the LUN from its iSCSI target. 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 or Windows 10.
- 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.
- **Allow symbolic links between different shared folders** must be enabled at **Control Panel** > **Network & File Services** > **Win/Mac/NFS** > **Microsoft Networking** > **Advanced Options** .

1. In Windows, open a NAS shared folder using File Explorer.
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.

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

Snapshot Clone

Cloning creates 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.

Cloning a Shared Folder

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.

Important
The shared folder have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Clone**.
   The **Clone Snapshot** window opens.
6. Specify a shared folder name.
7. Click **OK**.

Cloning a Block-Based LUN

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

Important
The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Clone**.
   The **Clone Snapshot** window opens.
6. Specify a LUN name.
7. Optional: Select an iSCSI target.
   QuTS hero will map the LUN copy to the target.
8. 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 a shared folder or block-based LUN to another storage pool, either on the same NAS or on a different QNAP NAS, using snapshots.
- Backing up data with Snapshot Replica reduces storage space and bandwidth requirements, and simplifies data recovery.

Protection Levels

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

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

Snapshot Replica Requirements

NAS	Requirement
Source and Destination NAS	Must be a QNAP NAS that supports snapshots.
Source and Destination NAS	Both source and destination NAS devices must be running QuTS hero. Replicating snapshots from QuTS hero to QTS or vice versa is not supported.
Source and Destination NAS	Must have at least 1GB of installed memory.

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

Creating a Snapshot Replica Job

Important
When running a Snapshot Replica job for the first time, all data on the 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 **Storage & Snapshots** > **Snapshot Backup** > **Snapshot Replica** .
2. Click **Create a Replication Job**.
   The **Create a Snapshot Replication Job** wizard opens.
3. Select the source shared folder or LUN.
4. Optional: Specify a job name.

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

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

Action	Destination NAS Location	Description
Manually specify the NAS address	LAN, WAN, Internet	Allows you to enter an IP address, hostname, or FQDN
Click **Detect** and then select a NAS from the list	LAN	Displays a list of all QNAP NAS devices on the local network
Click **Local Host**	Local NAS	Replicates snapshots between different storage pools on the same NAS

7. Specify an administrator account and password of the destination NAS.

Important
For security reasons, QNAP does not recommend using the "admin" account.

8. Optional: Specify a port.

Tip
The default port is 22.

9. Click **Test**.
   QuTS hero connects to the destination NAS using the specified admin password, and checks that there is sufficient storage space.

10. Click **Next**.
11. Specify how many replicated snapshots will be kept on the destination NAS.
    After the specified number is reached, QuTS hero will delete the oldest snapshot each time it replicates a new snapshot.
12. Select the destination storage pool.
13. Click **Next**.
14. Select a backup plan.

Backup Plan	Description
Start replication job after taking a local snapshot	The replica job will run each time QuTS hero creates the specified number of snapshots. These snapshots may be created manually or on a schedule.

Start replication job on a schedule	The replica job 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.
	Choose one of the following scheduling options, and then click **Add**.
	• Run on a schedule: The job automatically runs daily, weekly, or monthly. Settings:
	  • Schedule: How often the job runs
	  • Day: The day that the job runs on
	  • Expiration date: The replica job stops running after this date
	  • Frequency: How often the job runs on the days specified by "Schedule" and "Day"
	  • Start at: The time that the job starts running.
	• Run once: The job runs once on a specific time and day.
	• Manually start: The job does not run unless a user starts it.

Backup Plan	Description

Take a new snapshot on a schedule, then run replication job	The replica job runs according to the specified schedule. QuTS hero takes a new snapshot immediately before starting each run of the job. This ensures that there is always at least one snapshot to replicate. Choose one of the following scheduling options, and then click **Add**.
	• Run on a schedule: The job automatically runs daily, weekly, or monthly. Settings:
	  • Schedule: How often the job runs
	  • Day: The day that the job runs on
	  • Expiration date: The replica job stops running after this date
	  • Frequency: How often the job runs on the days specified by "Schedule" and "Day"
	  • Start at: The time that the job starts running.
	• Run once: The job runs once on a specific time and day.
	• Manually start: The job does not run unless a user starts it.

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

Setting	Description
Encrypt 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.
Compress 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 speed	Limits how much network bandwidth this job uses

17. Optional: Export the source data to an external storage device.
    To save time and bandwidth, you can export the source data to a connected external storage device such as a USB disk. After connecting the external storage device to the destination NAS, QuTS hero will import the source data when the job is next run.
    a. Connect an external storage device to the NAS.
    b. Select **Export source data to external storage device on first run**.
    c. Select the external storage device.

d. Optional: Select **Skip the export** if you have already exported the source data to the external storage device.

18. Click **Next**.
19. Optional: Select **Execute backup immediately**.
    When enabled, the job will run immediately after being created.
20. Review the job information.
21. Click **Finish**.
    QuTS hero creates the job.
22. Optional: If you chose to export source data to an external storage device, disconnect the storage device from the source NAS and connect it to the destination NAS.

Snapshot Replica Management

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

Snapshot Replica Job Actions

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

Snapshot Replica Options

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

Data Recovery on a Source NAS

Restoring Files and Folders from a Remote Snapshot

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

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

2. Select a shared folder.

Important
The shared folder must be the source folder for a Snapshot Replica job.

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

Action	Description
Select **Restore** > **Restore Files**	Restore the files or folders to their original storage location. If the files or folders still exists on the NAS, then they will be overwritten with the older versions. **Warning** All changes made after the snapshot was taken will be deleted.
Select **Restore** > **Restore Files to**	Choose one of the following restoration options. • Restore the files or folders to a different location on the NAS. • Restore the files or folders to remote mounted storage space. • Restore a single shared folder as a new shared folder.
In the menu bar, click	Download the files and folders to your computer in a ZIP file.

QuTS hero restores the files and folders then displays a confirmation message.

Reverting a Shared Folder Using a Remote Snapshot

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

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.

Important
The shared folder must be the source folder for a Snapshot Replica job.

3. Click **Snapshot**, and then select **Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.

5. Select a snapshot.
6. Click **Revert Folder Snapshot**.

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

7. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	QuTS hero takes a snapshot before starting the revert. This ensures that changes made to data since the snapshot was taken are not permanently lost.
Enable encryption during transfer	QuTS hero encrypts the snapshot before sending it for additional security.

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

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

The status of the shared folder changes to `Remote Reverting`. QuTS hero disables access to the shared folder until the revert process is finished.

Reverting a LUN Using a Remote Snapshot

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

Warning

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

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

Important
The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.

5. Select a snapshot.
6. Click **Revert LUN Snapshot**.

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

7. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	QuTS hero takes a snapshot before starting the revert. This ensures that changes made to data since the snapshot was taken are not permanently lost.
Enable encryption during transfer	QuTS hero encrypts the snapshot before sending it for additional security.
Re-map LUN to the same iSCSI target after revert	If enabled, QuTS hero automatically remaps the LUN to its current target after reverting. If disabled, you must manually remap the LUN after reverting.

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

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

QuTS hero unmaps the LUN from its iSCSI target. The status of the LUN changes to `Reverting`.

Cloning a Shared Folder from a Remote Snapshot

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

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Select a shared folder.

Important
The shared folder have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
   The **Snapshot Manager** window opens.
4. Under **Select snapshot location**, select a remote NAS.
5. Select a snapshot.
6. Click **Clone**.
   The **Clone Snapshot** window opens.

7. Specify a shared folder name.
8. Select a storage pool.
9. Optional: Select **Enable encryption during transfer**.
   QuTS hero encrypts the snapshot before sending it for additional security.
10. Click **OK**.

QuTS hero clones the shared folder, and then displays a confirmation message.

Cloning a Block-Based LUN from a Remote Snapshot

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

Important
The LUN must have at least one snapshot.

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

QuTS hero clones the LUN and then displays a confirmation message.

Data Recovery on a Destination NAS

Snapshot Vault

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

Restoring Files and Folders from a Snapshot Vault

1. Go to **Storage & Snapshots** > **Snapshot Backup** > **Snapshot Vault** .
2. Select a storage pool.
3. On a vault, click .
   The **Snapshot Vault** window opens.

4. Optional: Unlock the vault.
   If the original source shared folder is encrypted, you must unlock the vault with the shared folder's encryption password.
   a. Click **Unlock**.
   b. Enter the encryption password or upload the encryption key.
   c. Click **OK**.
5. Select a snapshot.
6. Select the files and folders to be restored.
7. Click **Restore Files To**.
8. Specify a restore location.
9. Click **OK**.

Cloning a Shared Folder from a Snapshot Vault

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

QuTS hero clones the shared folder, and then displays a confirmation message.

Cloning a Block-Based LUN from a Snapshot Vault

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

1. Go to **Storage & Snapshots** > **Snapshot Backup** > **Snapshot Vault** .
2. Select a storage pool.

3. On a vault, click .
   The **Snapshot Vault** window opens.
4. Select a snapshot.
5. Click **Clone**.
   The **Clone Snapshot** window opens.
6. Specify a LUN name.
7. Optional: Select an iSCSI target.
   QuTS hero will map the LUN copy to the target.
8. Click **OK**.

QuTS hero clones the LUN and then displays a confirmation message.

Cache Acceleration

Cache Acceleration enables you to create an SSD cache to improve the read and write performance of the NAS.

Cache Acceleration Requirements

- The NAS model must support Cache Acceleration.
  For information about NAS and drive bay compatibility, see https://www.qnap.com/solution/ssd-cache.
- The NAS must have one or more free SSDs installed in a compatible drive bay.
- The NAS must have a suitable amount of installed memory.
  The amount of memory required depends on the size of the SSD cache.

SSD Cache Size	Required Memory
512GB	≧ 1GB
1TB	≧ 4GB
2TB	≧ 8GB
4TB	≧ 16GB

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 & Snapshots** > **Storage** > **Cache Acceleration** .
2. Click .
   The **SSD Cache Introduction** window opens.
3. Click **Start**.
   The **Create SSD Cache** window opens.
4. Select one or more SSDs.

Warning
All data on the selected disks will be deleted.

5. Select a cache type.

Cache Type	Description
Read Cache	When data is read from a LUN or shared folder, QuTS hero copies the data to the SSD cache to speed up future read requests.
Read Cache and ZIL Synchronized Write Log	QuTS hero creates a read cache for accelerating read speeds, and also an SSD ZFS intent log (ZIL). The SSD ZIL is not a true write cache, but it can help accelerate random write performance.

6. Click **Next**.
7. Select which shared folders and LUNs can use the SSD cache.

Tip
This list can be modified later.

8. Click **Next**.
9. Select a cache mode.

Cache Mode	Description	Recommended Use Cases
Random I/O	Only small data blocks are added to the SSD cache. Larger blocks are accessed directly from regular storage.	Virtualization, databases
All I/O	Small and large data blocks are added to the SSD cache. Both sequential and random I/O requests are accelerated.	Video streaming, large file access operations

Tip
An HDD RAID group may outperform a SSD RAID group for sequential I/O if the ratio of HDDs to SSDs is 3:1 or greater, and the HDD group has a RAID type of RAID 0, 5, 6, or 10. However, SSDs will always be faster for random I/O. If the NAS contains a RAID group of type RAID 0, 5, 6, or 10 that contains three times more disks than the SSD cache, you should select **Random I/O**.

10. Click **Next**.
11. Review the summary information.
12. Click **Create**.
    A confirmation message appears.
13. 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 & Snapshots** > **Storage** > **Cache Acceleration** .
2. Click **Manage**, and then select **Configure Cache Disks**.
   The **Configure Cache Disks** window opens.

3. Select the SSDs to be included in the cache.

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

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

4. 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 & Snapshots** > **Storage** > **Cache Acceleration** .
2. Click **Manage**, and then select **Configure Cached Storage**.
3. Select the shared folders and LUNs that are allowed to use the SSD cache.

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

4. Click **Apply**.

Removing the SSD Cache

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

1. Go to **Storage & Snapshots** > **Storage** > **Cache Acceleration** .
2. Click **Manage** and then select **Remove**.
   A confirmation message appears.
3. Click **OK**.

QuTS hero flushes all data in the cache to disk, then deleted the RAID groups. This process make 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 & Snapshots** > **Storage** > **External Storage** . QuTS hero will also create a shared folder for each readable partition on the device.

Note
To access partitions formatted using the exFAT file system, you must purchase an exFAT driver license in License Center.

External Storage Device Actions

Action	Description
Erase	Delete all data and partitions on the device.
Eject	Safely unmount the external storage device from the NAS, so that you can disconnect it.

External Storage Disk Actions

Action	Description
Full Disk Format	Format the disk. For details, see Formatting an External Storage Partition.
Secure Erase	Permanently erase all data on a disk. For details, see Secure Erase.

External Storage Partition Actions

Action	Description
Storage Information	Displays details about the selected partition, including partition name, capacity, used space, and file system type.
Format	Formats the partition. For details, see Formatting an External Storage Partition.
Encryption Management	Manages encryption on a previously encrypted device. You can lock or unlock the device, change the encryption password, or download the encryption key.
Eject	Unmounts the partition. The external storage device and any stored partitions will continue working.

Formatting an External Storage Partition

1. Go to **Storage & Snapshots** > **Storage** > **External Storage** .
2. Select a storage partition.
3. Click **Action**, and then select **Format**.
   The **Format Partition** window opens.
4. Select a file system.

File System	Recommended Operating Systems and Devices
NTFS	Windows
HTS+	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** • Using exFAT on QuTS hero requires an exFAT driver license. You can purchase the license in License Center. • Verify that your device is compatible with exFAT before selecting this option.
EXT3	Linux, NAS devices
EXT4	Linux, NAS devices

5. 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 "-"
6. Optional: Enable encryption.
   a. Select an encryption type.
      Select one of the following options:
      - AES 128 bits
      - AES 192 bits
      - AES 256 bits
   b. Specify an encryption password.
      The password must consist of 8 to 16 characters from any of the following groups:
      - Letters: A to Z, a to z
      - Numbers: 0 to 9
      - All special characters (excluding spaces)
   c. Confirm the encryption password.
   d. Optional: Select **Save encryption key**.
      Select this option to save a local copy of the encryption key on the NAS. This enables 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, the volume 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 **Shared Folders** 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 & Snapshots** > **Storage** > **Remote Disk** .
2. Click **Add Virtual Disk**.
3. Specify the IP address or hostname of the remote server.
4. Optional: Specify the iSCSI port of the remote server.
5. Click **Get Remote Disk**.
   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
HTS+	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. Click **Finish**.

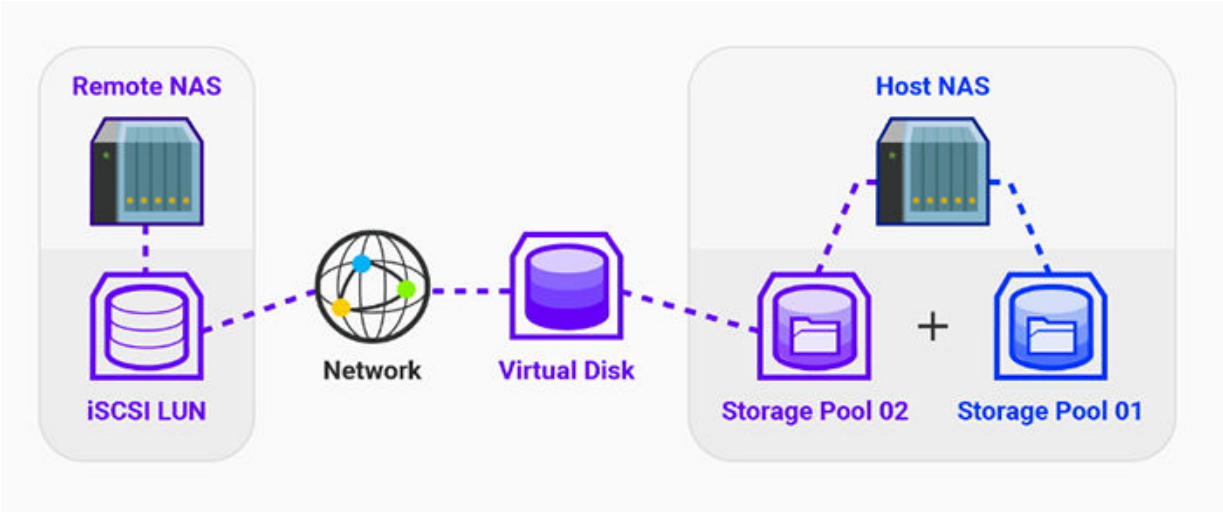
QuTS hero adds the remote disk and shares it at **Control Panel** > **Privilege** > **Shared Folders** . By default only the admin account has access.

Remote Disk Actions

Action	Description
Edit	Edit the name of the disk.
Delete	Disconnect the remote disk and delete its shared folder. Existing data on the disk will not be deleted.
Format	Format the remote disk. Select one of the following file system options: • ext4 • ext3 • FAT32 • NTFS • HTS+ Select one of the following I/O options: • Synchronous • Asynchronous

VJBOD (Virtual JBOD)

VJBOD (Virtual JBOD) enables you to add storage space from other QNAP NAS devices to your NAS as local VJBOD disks, to create a virtual expansion enclosure. VJBOD disks can be used to create new local storage space, expanding local NAS storage capacity. VJBOD is based on iSCSI technology.



VJBOD Requirements

Local NAS requirements:

- The NAS is running QTS 4.2.2 or later, or QuTS hero 4.5.0 or later.
- The NAS model supports VJBOD.

For a list of supported series and models, see https://www.qnap.com/solution/vjbod.

Remote NAS requirements:

- The NAS is running QTS 4.2.1 or later, or QuTS hero.
- The NAS model supports iSCSI and storage pools.
- The NAS has a storage pool with at least 154 GB of free space, or an unused thick LUN with a capacity of 154 GB or more.

Tip
For a stable VJBOD connection, ensure the following conditions:

- All NAS devices are on the same local network.
- All NAS devices are configured with static IP addresses.
- On a remote NAS, additional LUNs are not mapped to an iSCSI target that is being used by a VJBOD disk.

VJBOD Limitations

- You can create a maximum of 8 VJBOD disks.
- You can only expand an existing storage pool using VJBOD disks if the pool consists of VJBOD disks from the same storage pool on the same remote NAS.
- 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 of IP blocks
  - Incorrect CHAP credentials

VJBOD Creation

Creating a VJBOD Disk from a New LUN

1. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .
2. Click **Create**, and then select **Create Virtual JBOD**.
   The **Create Virtual JBOD Disk Wizard** opens.

3. Click **Next**.
4. Specify the IP address or hostname of the remote NAS.

Important
The remote NAS must have at least one storage pool containing at least 153 GB of free space.

Tip
Click **Detect** to view the IP addresses of all QNAP NAS devices on the local network. Click **Local Host** to use the IP of the local NAS.

5. Specify an administrator account and password of the remote NAS.

Important
For security reasons, QNAP does not recommend using the "admin" account.

6. Optional: Specify the system administration port of the remote NAS.

Tip
The default port is 8080. If HTTPS is enabled, the default port is 443.

7. Click **Next**.
8. Optional: Select the local interface that will be used by VJBOD.
9. Optional: Select the remote interface that will be used by VJBOD.
10. 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**.
11. Click **Next**.
12. Select **Create a new iSCSI LUN on the remote NAS**.
13. 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.

14. Click **Next**.
15. Select a storage pool.
16. Click **Next**.
17. Specify the capacity of the VJBOD disk.

Important
The size of the VJBOD disk cannot be changed after creation.

18. Optional: Configure advanced settings.

Setting	Description
SSD cache	The SSD cache will be used to improve VJBOD disk access performance.

19. Click **Next**.
    QuTS hero starts creating a dedicated iSCSI target on the remote NAS for the VJBOD disk.
20. 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
21. 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.

22. Click **Next**.
23. Review the summary, and then click **Next**.
    QuTS hero creates the iSCSI target and LUN on the remote NAS, and then creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
24. 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`.

25. Click **Finish**.

Creating a VJBOD Disk from an Existing LUN

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

2. Click **Create**, and then select **Create Virtual JBOD**.
   The **Create Virtual JBOD Disk Wizard** opens.
3. Click **Next**.
4. Specify the IP address or hostname of the remote NAS.

> **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 **Next**.
8. Optional: Select the local interface that will be used by VJBOD.
9. Optional: Select the remote interface that will be used by VJBOD.
10. 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**.
11. Click **Next**.
12. Select **Choose an existing iSCSI LUN on the selected NAS**.
13. Click **Next**.
14. Select a LUN.

> **Important**
> The LUN must be thick and block-based, and must have a capacity of at least 154 GB. Mutual CHAP must be disabled.

15. Click **Next**.
16. 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

17. 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.

18. Click **Next**.
19. Review the summary, and then click **Next**.
    QuTS hero creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
20. Select a follow-up action.

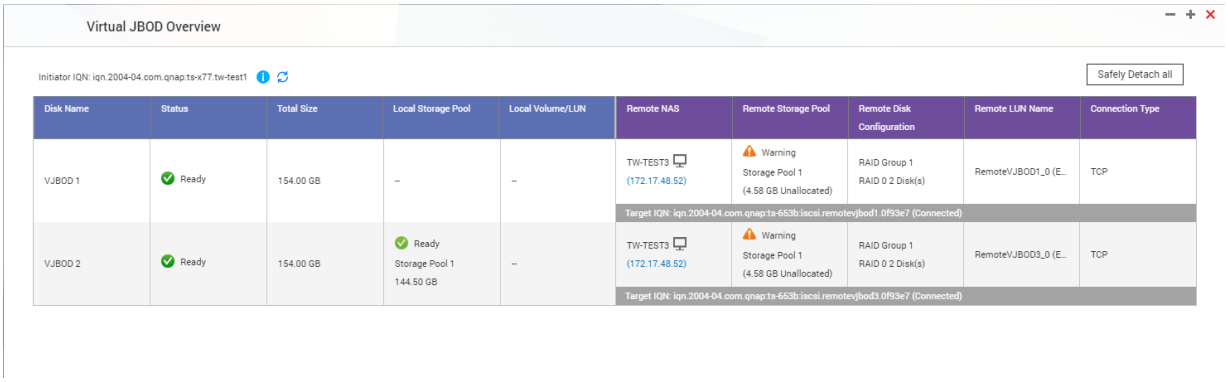
Action	Description
Create New Storage Pool	Creates a storage pool using the VJBOD disk
Recover Existing Data	Restores a storage pool that was previously created on the VJBOD disk
Do nothing	Ends the creation process. You can configure the VJBOD disk later. **Tip** To create a storage pool on a VJBOD disk later, go through the normal steps of creating a storage pool. Then on the disk selection screen, under **Enclosure Unit** select `Virtual JBOD`.

21. Click **Finish**.

VJBOD Management

Virtual JBOD Overview

To view an overview of all VJBOD disks including information on their source remote NAS devices, go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** , click **VJBOD**, and then select **VJBOD Overview**.



VJBOD Disk Actions

Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** , select a VJBOD disk, and then click **Action**.

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 a disconnected VJBOD disk
Edit Target	Disconnected	Edits the following iSCSI target settings: port number, CHAP authentication, and CRC checksum settings
Detach	Data	Safely disconnects the VJBOD disk containing a storage pool. You can then connect the LUN to another NAS, create a new VJBOD disk, and recover the pool using **Action** > **Data Recovery** .
Delete	Disconnected	Deletes a VJBOD from the local disk. The LUN and all data will remain on the remote NAS You can also choose to delete the iSCSI target and LUN on the remote NAS.

Moving a VJBOD Disk to Another QNAP NAS

1. Note the details of the VJBOD disk's remote LUN.
   a. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .
   b. Click **VJBOD**, and then select **VJBOD Overview**.
   The **VJBOD Overview** window opens.
   c. Locate the VJBOD disk that you want to move, and then note the **Remote LUN Name** and the IP address under **Remote NAS**.
2. Detach the VJBOD disk's storage pool.
   a. Go to **Storage & Snapshots** > **Storage** > **Storage/Snapshots** .

b. Select the storage pool on the VJBOD disk.

c. Click **Manage**.
The **Storage Pool Management** window opens.

d. Click **Action**, and then select **Safely Detach**.

3. Remove the VJBOD disk from the NAS.

a. Go to **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .

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 & Snapshots** > **Storage** > **Disks/VJBOD** .

b. Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.

c. Click **Next**.

d. Specify the IP address or hostname of the remote NAS.

e. Specify an administrator account and password of the remote NAS.

Important
For security reasons, QNAP does not recommend using the "admin" account.

f. Optional: Specify the system administration port of the remote NAS.

Tip
The default port is 8080. If HTTPS is enabled, the default port is 443.

g. Click **Next**.

h. Optional: Select the local interface that will be used by VJBOD.

i. Optional: Select the remote interface that will be used by VJBOD.

j. Optional: Select **Use iSER when available**.
Enabling iSER increases data transfer speeds and reduces CPU and memory load.

k. Click **Next**.

l. Select **Choose an existing iSCSI LUN on the selected NAS**.

m. Click **Next**.

n. Select the LUN containing the VJBOD disk.

o. Click **Next**.

p. 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.

q. Click **Next**.

r. Review the summary, and then click **Next**.
QuTS hero creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots** > **Storage** > **Disks/VJBOD** .

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

t. 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.

Installation

VJBOD Cloud Requirements

Requirements:

- A QNAP NAS running QuTS hero 4.5.1 or later
- A cloud space (bucket or container) with at least 1 GB of free space from a supported cloud service provider

Installing VJBOD Cloud

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.
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.

Limit	Amount	Notes
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.
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.

Cloud Service	Steps
Amazon S3	**1.** Select **AmazonS3**. **2.** Select a cloud service: • **AWS Global** • **AWS China** • **AWS GovCloud (US)**: Select either **Standard** or **FIPS** protocol. • **S3 Compatible**: Specify the server address. **3.** Specify the access key. **4.** Specify the secret key. **5.** Optional: Select **Enable secure connection (SSL)**. **6.** Optional: Select **Validate SSL certificate**.
Microsoft Azure	**1.** Select **Azure**. **2.** Specify the storage account. **3.** Specify the access key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
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**.

Cloud Service	Steps
Cynny Space	**1.** Select **Cynny Space**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
DigitalOcean	**1.** Select **Digital Ocean**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Select a region.
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**.
IBM Cloud	**1.** Select **IBM Cloud**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.

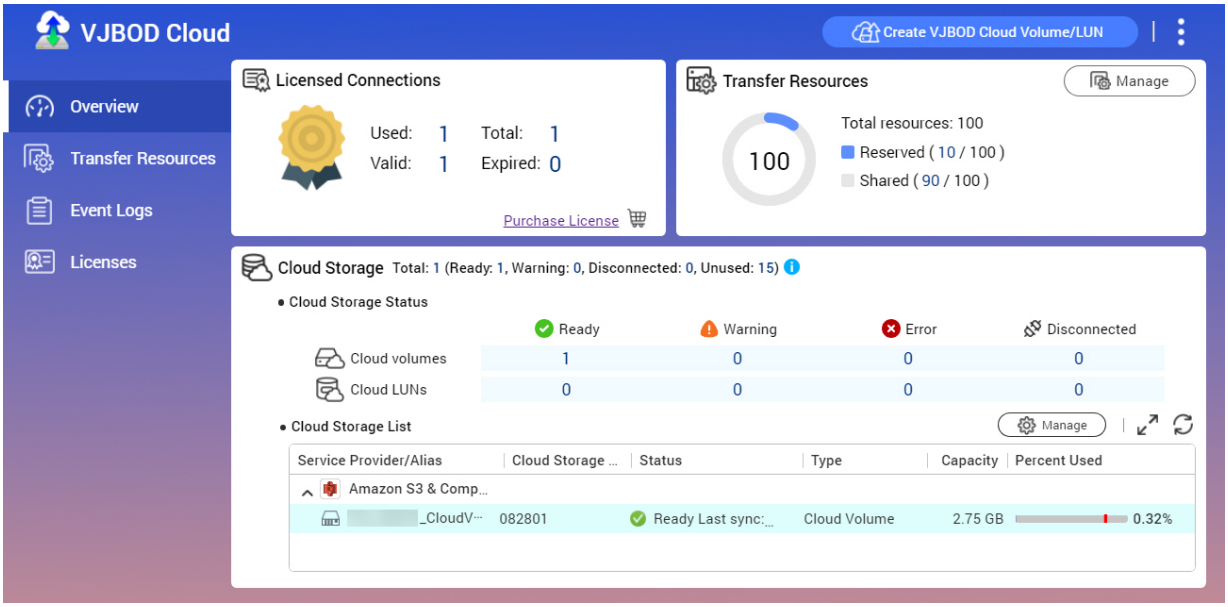
Cloud Service	Steps
luckycloud S3	**1.** Select **luckycloud S3**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Validate SSL certificate**.
Oracle Cloud	**1.** Select **Oracle Cloud**. **2.** Specify the name space. **3.** Specify the access key. **4.** Specify the secret key. **5.** Optional: Select **Enable secure connection (SSL)**. **6.** Optional: Select **Validate SSL certificate**. **7.** Select a region.
Qcloud Italy	**1.** Select **Qcloud IT**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Optional: Select **Enable secure connection (SSL)**. **5.** Optional: Select **Validate SSL certificate**.
Rackspace	**1.** Select **Rackspace**. **2.** Specify the user ID. **3.** Specify the password. **4.** Optional: Select **Validate SSL certificate**. **5.** Select a region.

Cloud Service	Steps
S3 Compatible	**1.** Select **S3 Compatible**. **2.** Specify the access key. **3.** Specify the secret key. **4.** Specify the authentication service. **5.** Select a signature version. **6.** Optional: Select **Enable secure connection (SSL)**. **7.** Optional: Select **Validate SSL certificate**. **8.** Optional: Specify a region.
Swift	**1.** Select **Swift**. **2.** Optional: Enable keystone authentication. **a.** Select **Enable Keystone Auth**. **b.** Specify a tenant ID or tenant name. **3.** Select the large object type. **4.** Specify the user ID. **5.** Specify the auth service. **6.** Specify the API key or password. **7.** Optional: Select **Validate SSL certificate**.
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.

Cloud Service	Steps
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**.

Overview

The **Overview** screen displays the number of used and total licensed connections, transfer resource information, and information on connected VJBOD Cloud volumes and LUNs. On this screen you can manage VJBOD Cloud volumes and LUNs by selecting one and then clicking **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**.

Action	Description	Steps
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 VJBOD Cloud Volume and LUN Recovery.

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 VJBOD Cloud Volume and LUN Recovery.

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.

Status	Description
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.

VJBOD Cloud Volume and LUN Recovery

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.

Recovering a VJBOD Cloud Volume or LUN

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.

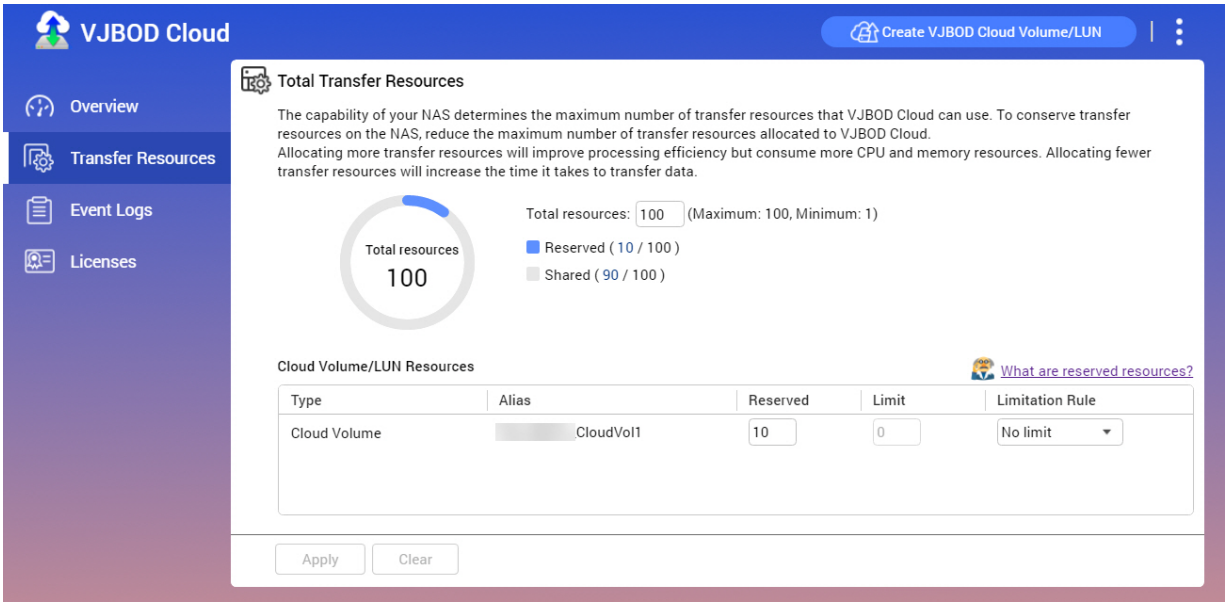
Warning
All changes to data made after the recovery point will be deleted.

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

The **Transfer Resources** screen displays the total number of transfer resources allocated to VJBOD Cloud, and the number of transfer allocated to each VJBOD Cloud volume and LUN. On this screen you can manage transfer resources allocation.



Transfer Resource Overview

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.

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.
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 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.

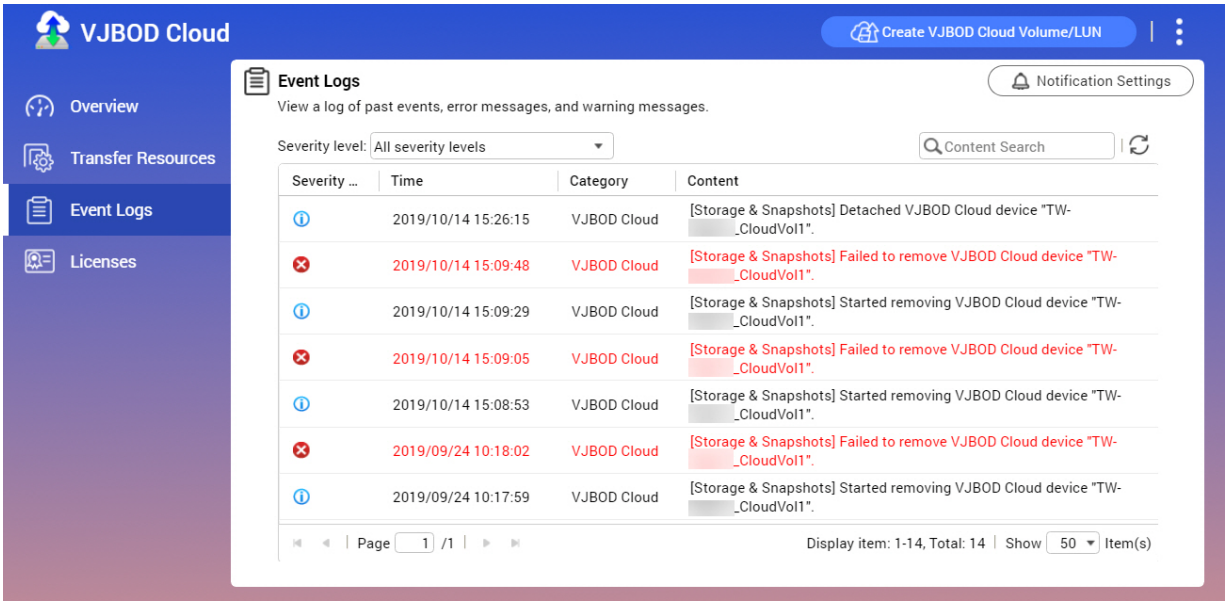
Setting	Description
Reserved	The number of transfer resources reserved for this volume or LUN.
Limit	The maximum number of transfer resources this volume or LUN can use. **Note** To set this value, **Limitation Rule** must be set to `Limit`.

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**.

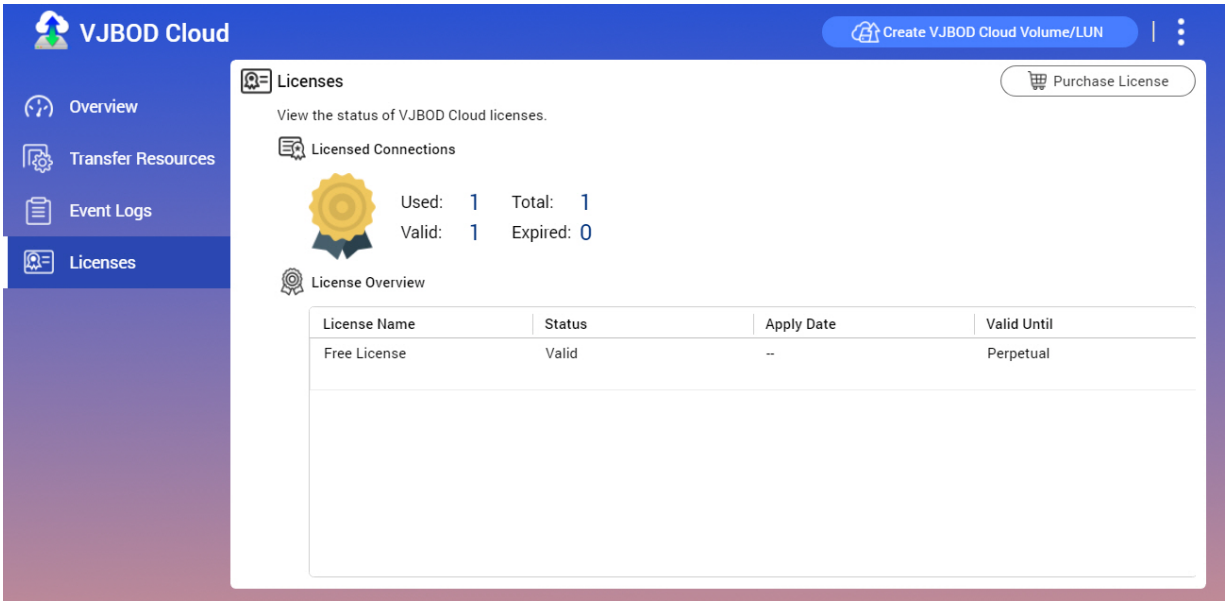
Event Logs

The **Event Logs** screen displays a log of events, error messages, and warnings related to VJBOD Cloud. On this screen you can view logs by severity level, search logs using keywords, and configure notification settings.



Licenses

The **Licenses** screen displays information about VJBOD Cloud licenses on the NAS. On this screen you can view how many 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

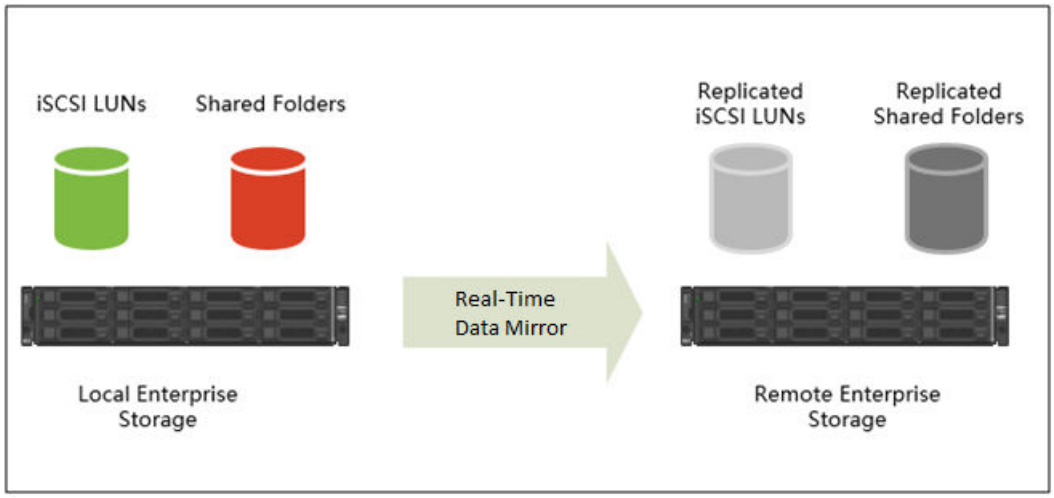
- VJBOD Cloud requires a license for each connection to a unique cloud space. A cloud space may be called a bucket, container, account name, or something else depending on the cloud service provider. For example, the following VJBOD Cloud volumes and LUNs require three licenses:
  - *Amazon S3 → Bucket1 → 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.

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

- You can also configure SnapSync to run periodically on a schedule (Scheduled SnapSync), in order to save system resources.
- 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 4.5.2 or later
QES to QuTS hero QuTS hero to QES	QES 2.1.1 Build 20210303 or later	QuTS hero 4.5.2 or later

Other requirements:

- The source and destination shared folder or LUN must be the same provisioning type (thick or thin).
- If the source and destination NAS devices are running incompatible versons of SnapSync, then you will be prompted to update the system firmware on one or both NAS devices.
- If both the source and destination NAS devices are running QES, then they must run the same version of QES to ensure data consistency.
- When using real-time SnapSync, the round-trip latency between the source and destination NAS devices must be 5ms or less. Higher latency might cause local storage write delays.

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

SnapSync Job Creation

The following options are available when creating a SnapSync job.

Option	Source NAS	Destination NAS	Use Cases
Create a SnapSync Backup Job to a Remote NAS	Local NAS	Remote NAS	Back up local NAS data.
Create a SnapSync Backup Job from a Remote NAS	Remote NAS	Local NAS	• Back up remote NAS data. • Restore previously backed up data to the local NAS.

Creating a SnapSync Job to a Remote NAS

1. Go to **Storage & Snapshots** > **Snapshot Backup** > **SnapSync** .
2. Click **Create a SnapSync Job**.
3. Click **Sync to Remote**.
   The **Create a SnapSync Job** wizard opens.
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.
7. Click **Next**.
8. Select the destination remote NAS.
9. Optional: Specify the remote SnapSync port number.

Note
The default is 8080.

10. Optional: Enable HTTPS encryption.
11. Specify an administrator account and password of the remote NAS.

Important
For security reasons, QNAP does not recommend using the "admin" account.

12. Click **Connect**.
13. Select a backup plan.

Backup Plan	Description
Scheduled	SnapSync backs up data periodically, according to a schedule. You can set the schedule to daily, weekly, or monthly. On the day the job runs, you can set the job to run once or periodically.
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.

14. Select the destination storage pool.
15. Select the destination shared folder or LUN.

Warning
All data in the shared folder will be deleted.

16. Optional: Click **New** to create a new destination shared folder.
17. Optional: Configure job options.

Setting	Description
Compression	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 connecting via WAN.
Deduplication	SnapSync reduces the amount of storage and bandwidth needed by eliminating duplicate copies of repeated data.
Encryption	SnapSync encrypts the data during transmission to the destination NAS. The data is then decrypted before being stored at the destination.

Setting	Description
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. You must install QNAP Snapshot Agent on the iSCSI initiator.

18. Click **Next**.
19. Set the source and destination network adapters for this job.

Adapter Setting	Description
Auto-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.
Manual-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 adapter lists are automatically filtered to only display adapters that can connect to the currently selected adapter.

20. Click **Next**.
21. Optional: Select **Execute backup immediately**.
    When selected, the job will run immediately after it has been created.
22. Click **Create**.

Creating a SnapSync Job from a Remote NAS

1. Go to **Storage & Snapshots** > **Snapshot Backup** > **SnapSync** .
2. Click **Create a SnapSync Job**.
3. Click **Sync from Remote**.
   The **Create a SnapSync Job** wizard opens.
4. Specify a job name.
   The name cannot contain any of the following special characters: ` * = + [ ] \ | ; : ' " , < > / ? %
5. Select the source remote NAS.
6. Optional: Specify the remote SnapSync port number.

Note
The default is 8080.

7. Specify an administrator account and password of the remote NAS.

Important
For security reasons, QNAP does not recommend using the "admin" account.

8. Click **Connect**.
9. Select the source storage pool.
10. Select the source shared folder or LUN.
11. Select the destination storage pool.
12. Select the destination shared folder or LUN.

Warning
All data in the shared folder will be deleted.

13. Optional: Click **New** to create a new destination shared folder.
14. Click **Continue on Remote NAS**.
    The SnapSync wizard opens on the remote NAS.
15. Select a backup plan.

Backup Plan	Description
Scheduled	SnapSync backs up data periodically, according to a schedule. You can set the schedule to daily, weekly, or monthly. On the day the job runs, you can set the job to run once or periodically.
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.

16. Configure settings for the destination NAS.
    The destination NAS is the NAS you started creating this job on.
    a. Specify the remote SnapSync port number.

Note
The default is 8080.

    b. Enter the remote NAS admin username and password.
    c. Click **Connect**.
    d. Select the destination storage pool.
    e. Select the destination shared folder or LUN.

Warning
All data in the shared folder will be deleted.

17. Optional: Configure job options.

Setting	Description
Compression	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 connecting via WAN.
Deduplication	SnapSync reduces the amount of storage and bandwidth needed by eliminating duplicate copies of repeated data.
Encryption	SnapSync encrypts the data during transmission to the destination NAS. The data is then decrypted before being stored at the destination.
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. You must install QNAP Snapshot Agent on the iSCSI initiator.

18. Click **Next**.
19. Set the source and destination network adapters for this job.

Adapter Setting	Description
Auto-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.
Manual-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 adapter lists are automatically filtered to only display adapters that can connect to the currently selected adapter.

20. Click **Next**.
21. Optional: Select **Execute backup immediately**.
    When selected, the job will run immediately after it has been created.
22. Click **Create**.

SnapSync Screen

To get to this screen, go to **Storage & Snapshots** > **Snapshot Backup** > **SnapSync** .

SnapSync Screen UI Elements

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.

UI Element	Description
Port	Displays the port used for incoming and outgoing SnapSync connections.
SnapSync Settings	Set the SnapSync port and limit upload rate. For details, see SnapSync Settings.
Create a SnapSync Job	Create a real-time or scheduled SnapSync job. For details, see Creating a SnapSync Job to a Remote NAS.
Job Name	Displays the job's name.
Source	Displays the following information: • Source NAS name • Source shared folder or LUN name • Source interface IP address • Source link and adapter speed
Destination	Displays the following information: • Destination NAS name • Destination shared folder or LUN name • Destination interface IP address • Destination link and adapter speed
Compression	Displays whether compression is enabled for this job.
Deduplication	Displays whether deduplication is enabled for this job.
Backup Plan	Displays the backup plan for this job: • Manual • Scheduled • Real-time
State	Displays the current job status. For details, see the following topics: • Real-Time SnapSync Job Status • Scheduled SnapSync Job Status If QuTS hero is unable to contact the remote NAS, this field displays the last known job status plus `(Disconnected)`. If the job is running, this field also shows job speed real-time and scheduled jobs, and percentage completed for scheduled jobs.
Run now	Run the job now if it is not yet running.
Action	Edit, delete, or resume the job. For details, see SnapSync Job Actions.

SnapSync Settings

UI Element	Action
SnapSync version	This displays the SnapSync version on the current NAS firmware. **Tip** If you are having SnapSync compatibility issues, ensure that both source and destination NAS devices have the same SnapSync version.
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.
Maximum upload rate (KB/s)	Set the maximum upload rate for SnapSync, in kilobytes per second. 0 is unrestricted.

SnapSync Job Actions

Action	Description
Edit	Edit the job's settings. You can edit backup frequency, network adapter, and certain job options. **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 destination login account password changes, then the job will stop working. To resolve this issue, edit the job setting on the source NAS and then update the destination password. • 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.
Suspend job	Temporarily prevents a job from running as scheduled.
Resume job	Allows a previously suspended job to run as scheduled. If QuTS hero detects that the source and destination folders are different, then it immediately runs the job and synchronizes them.

Scheduled SnapSync Job Status

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.

Status	Description
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

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.
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 might be either consistent or inconsistent.
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

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.

7. iSCSI & Fibre Channel

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 access global settings by clicking in the **iSCSI & Fibre Channel** window.

Setting	Description
Enable iSCSI and Fibre Channel services	Enable these services to use iSCSI and Fibre Channel on your NAS.
iSCSI service port	View and modify the port that iSCSI initiators connect to. **Tip** The default port is 3260.
Enable iSNS	SNS enables the automatic discovery and management of iSCSI initiators and targets within a TCP/IP network. **iSNS server IP**: Specify the IP address of the iSNS server.

Creating a Block-Based LUN

1. Go to one of the following screens.
   - **iSCSI & Fibre Channel** > **iSCSI Storage**

- **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage**

2. Click **Create**, and then select **New Block-Based LUN**.
   The **Create LUN** window opens.
3. Specify a LUN name
   - Length: 1 to 32 characters
   - Valid characters: 0-9, a-z, A-Z, underscore (_)
4. Select the storage pool that this LUN will be created in.
5. 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.

6. Specify a LUN capacity.
   Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method:
   - Thick provisioning: Equal to the amount of free space in the parent storage pool.
   - Thin provisioning: 1 PB
7. Optional: Configure LUN guaranteed snapshot space.
   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.
8. Optional: Configure the following LUN 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 filesystems. 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 8 GB of memory.
Alert threshold	QuTS hero issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold.

Setting	Description
SSD Cache	The SSD cache will be used to improve LUN access performance. **Important** This setting is only available when the SSD cache is enabled.
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.
Synchronous I/O	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: (Default). 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.

9. Optional: Select **Map LUN to an iSCSI target or FC port group**
   If selected, the **Edit LUN Mapping** wizard appears after QuTS hero has finished creating the LUN.
10. Click **Create**
11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.
    For details, see the following topics:
    - Mapping a LUN to an iSCSI Target
    - Mapping a LUN to a Fibre Channel Port Group

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 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 Storage

The **iSCSI Storage** screen allows you to view iSCSI targets. On this screen you can enable, disable, and edit targets, view each target's mapped LUNs, edit LUN mappings, take snapshots of LUNs, and configure the ISCSI access control list (ACL).

Note
The **Allocated** column displays the space consumption of each LUN. Differences in calculation methods may result in different allocated space values on the NAS and the LUN host.

iSCSI LUNs

Mapping a LUN to an iSCSI Target

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Select a LUN.

> **Tip**
> Double-click an iSCSI target to view all of its mapped LUNs.

3. Optional: If the LUN is already mapped to a target, disable the LUN.
   a. Click **Action**, and then select **Disable** .
   A confirmation message appears.
   b. Click **OK**.
   QuTS hero disables the LUN.
4. Click **Action**, and then select **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
5. Select **Map to iSCSI target**.
6. Select an iSCSI target.
7. Optional: Select **Enable LUN**.
   If selected, QuTS hero will enable the LUN after mapping it to the target.
8. Click **OK**.

iSCSI LUN Actions

LUN Action	Description
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.
Enable	Enable the LUN if it is currently disabled.
Modify	Edit the LUN settings.
Delete	Delete the LUN and all data stored on it. **Important** • This action is only available if the LUN is unmapped. • To delete a VJBOD Cloud LUN, use the VJBOD Cloud app.
Edit LUN Mapping	Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: • Mapping a LUN to a Fibre Channel Port Group • Mapping a LUN to an iSCSI Target
Show in Storage & Snapshots	Manage the LUN at **Storage & Snapshots** > **Storage** > **Storage/ Snapshots**

LUN Action	Description
LUN Import/Export	Export the LUN to another server, a local NAS folder, or an external storage device. For details, see Creating a LUN Export Job.

iSCSI LUN Status

Status	Description
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.

iSCSI Targets

Creating an iSCSI Target

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Click **Create**, and then select **New iSCSI Target**.
   The **iSCSI Target Creation Wizard** window opens.
3. Click **Next**.
4. Specify a target name.
   QuTS hero appends the specified name to the iSCSI qualified name (IQN). IQNs are unique names used to identify targets and initiators.
   - Valid characters: 0 to 9, a to z, A to Z
   - Length: 1 to 16 characters
5. Optional: Specify a target alias.
   An alias enables you to identify the target more easily on the initiator.
   - Length: 1 to 32 characters
   - Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ( )
6. Optional: Select **Allow clustered access to this target**.
   When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously.

Warning
To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.

7. Optional: Enable CRC checksums.
   Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

8. Click **Next**.

9. 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
10. Optional: Enable mutual CHAP authentication.
    Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.
    - Username
      - Length: 1 to 127 characters
      - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
    - Password
      - Length: 12 to 16 characters
      - Valid characters: 0 to 9, a to z, A to Z, all special characters
11. Click **Next**.
12. Optional: Select **Create a LUN and map it to this target**.
    If selected, QuTS hero opens the **Block-Based LUN Creation Wizard** immediately after finishing this wizard. The new LUN will then be automatically mapped to this target.
13. Click **Apply**.

QuTS hero creates the iSCSI target, and then opens the **Block-Based LUN Creation Wizard** window if **Create an iSCSI LUN and map it to this target** was enabled.

Editing iSCSI Target Settings

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify iSCSI Target** window opens.
4. Modify any of the following settings.

Setting	Description
Target Alias	An alias enables you to identify the target more easily on the initiator. • Length: 1 to 32 characters • Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ( )
Enable clustered access to the iSCSI target from multiple initiators	When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously. **Warning** To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.
CRC/Checksum	Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately. • Data Digest: The checksum can be used to verify the data portion of the PDU. • Header Digest: The checksum can be used to verify the header portion of the PDU.

Use CHAP 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

Mutual CHAP	Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.
	• Username
	  • Length: 1 to 127 characters
	  • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
	• Password
	  • Length: 12 to 16 characters
	  • Valid characters: 0 to 9, a to z, A to Z, all special characters

5. Click **Apply**.

iSCSI Target Actions

Action	Description
Deactivate	Disable an active target and disconnect all connected iSCSI initiators.
Activate	Enable a deactivated target.
Modify	Edit the target's settings. For details, see Editing iSCSI Target Settings.
View Connections	View the IP addresses and IQN information of all iSCSI initiators connected to this target.
Delete	Disconnect all connected iSCSI initiators and delete the target. Any LUNs mapped to the target will be unmapped and then added to the unmapped LUN list.

iSCSI Target Status

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 ACL

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 Storage** .
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.
3. Click **Add a Policy**.
   The **Add a Policy** window opens.
4. Specify the policy name.
   The name must consist of 1 to 32 characters from any of the following groups:
   - Letters: a-z, A-Z
   - Numbers: 0-9
   - Special characters: Hyphen (-), space ( ), underscore (_)

5. Specify the initiator IQN.
6. Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

Tip
Click the values in the columns to change the permissions.

7. Click **Apply**.

Editing an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.
3. Select a policy.
4. Click **Edit**.
   The **Modifiy a Policy** window opens.
5. Optional: Edit the policy name.
   The name must consist of 1 to 32 characters from any of the following groups:
   - Letters: a-z, A-Z
   - Numbers: 0-9
   - Special characters: Hyphen (-), space ( ), underscore (_)
6. Optional: Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

Tip
Click the values in the columns to change the permissions.

7. Click **Apply**.

Deleting an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Click **iSCSI ACL**.
   The **iSCSI ACL** window opens.

3. Select a policy.
4. Click **Delete**.
   A confirmation message appears.
5. Click **OK**.

iSCSI Target Authorization

Each iSCSI target can be configured either to allow connections from all iSCSI initiators, or to only allow connections from a list of authorized initiators.

Important
By default, iSCSI target authorization is disabled.

Configuring an iSCSI Target's Authorized Initiators List

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow connections from the list only**.
6. Optional: Add one or more iSCSI initiators to the authorized iSCSI initiators list.
   a. Click **Add**.
   b. Specify the initiator IQN.
   c. Click **Confirm**.
   d. Repeat the previous steps for each additional iSCSI initiator that you want to add.
7. Optional: Delete one or more iSCSI initiators from the authorized iSCSI initiators list.
   a. Select an initiator IQN.
   b. Click **Delete**.
   c. Repeat the previous steps for each additional iSCSI initiator that you want to delete.
8. Click **Apply**.

Enabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow connections from the list only**.

6. Add one or more iSCSI initiators to the authorized iSCSI initiators list.
   a. Click **Add**.
   b. Specify the initiator IQN.
   c. Click **Confirm**.
7. Repeat the previous steps for each additional iSCSI initiator that you want to add.
8. Click **Apply**.

Disabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel** > **iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
   The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow all connections**.
6. Click **Apply**.

QNAP Snapshot Agent

QNAP Snapshot Agent enables QuTS hero to take application-consistent snapshots of iSCSI LUNs on VMware or Microsoft servers. Application-consistent snapshots record the state of running applications, virtual machines, and data. When QuTS hero takes a LUN snapshot, QNAP Snapshot Agent triggers the following actions:

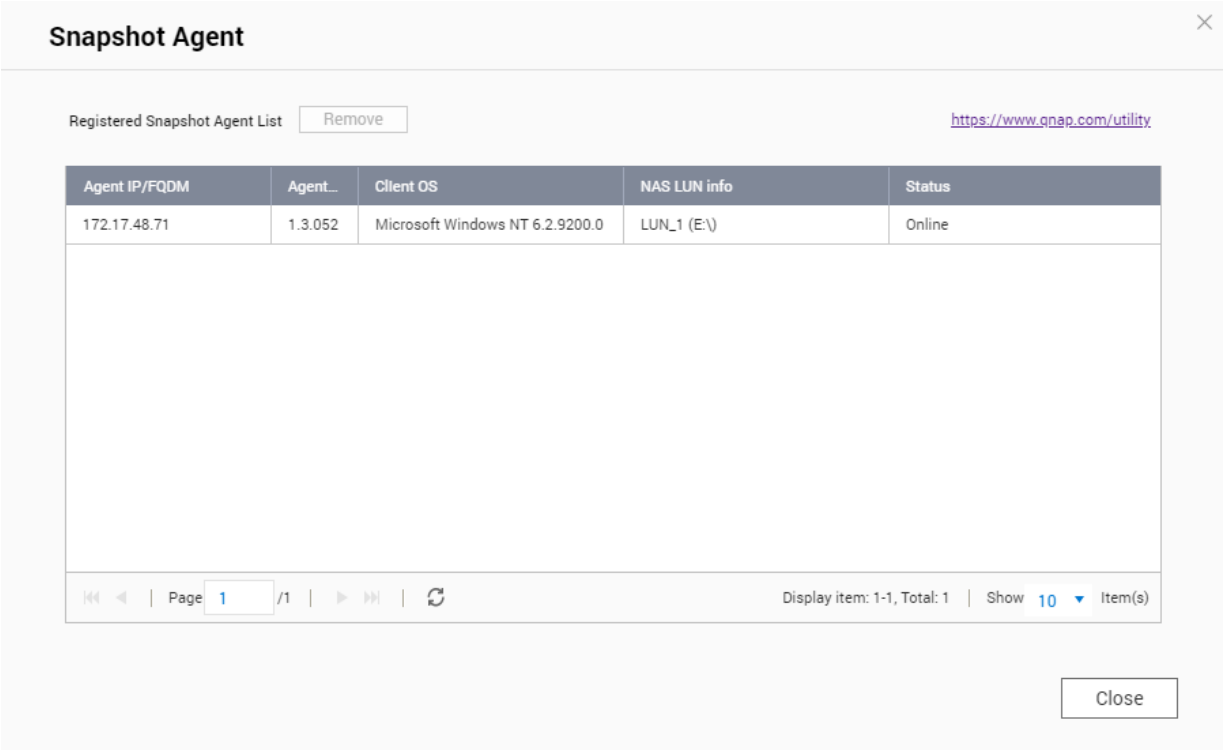
- Windows: The server flushes data in memory, logs, and pending I/O transactions to the LUN before the snapshot is created.
- VMware: The server takes a virtual machine snapshot.

> **Tip**
> To download QNAP Snapshot Agent, go to https://www.qnap.com/utilities.

Snapshot Agent Server List

To view a list of all iSCSI initiators that are using QNAP Snapshot Agent with this NAS, go to **iSCSI & Fibre Channel** > **iSCSI Storage** . Click **Snapshot**, and then select **Snapshot Agent**.

> **Tip**
> To unregister an iSCSI initiator, select it in the list and then click **Remove**.



Fibre Channel

FC Ports

The **Fibre Channel (FC) Ports** screen displays all of the Fibre Channel ports and port groups on the NAS.

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 Chanel group.
- There is a default port group that contains all Fibre Channel ports.

Creating a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports** .
2. Click **Create Port Group**.
   The **Create Port Group** window opens.
3. Specify a group name.
   Name requirements:
   - Length: 1–20 characters

- Valid characters: A–Z, a–z, 0–9

4. Select one or more Fibre Channel ports.
5. Click **Create**.

Mapping a LUN to a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage** .
2. Select a LUN.
3. Click **Action**, and then select **Edit LUN Mapping**.
   The **Edit LUN Mapping** window opens.
4. Select **Map to FC port group**.
5. Select a Fibre Channel port group.

Tip
The default group contains all Fibre Channel ports.

6. Choose whether you want to configure LUN masking.

Option	Description
Enable LUN and do not configure LUN masking	Do not configure LUN masking. Any initiator that is able to connect to a Fibre Channel port in the port group will be able to see the LUN.
Keep LUN disabled and configure LUN masking in the next step	Configure LUN masking. You can restrict which initiators can see the LUN.

7. Click **OK**.
8. Optional: Configure LUN masking.
   a. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	1. Select one or more initiator WWPNs in the WWPN list. 2. Click **Add**.
Add WWPNs as text	1. Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` 2. Click **Add**.

   b. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .

   c. Optional: Select **Enable LUN**.
   If selected, QuTS hero will enable the LUN after mapping it to the target.

   d. Click **OK**.

Fibre Channel Port Actions

Action	Description
Edit Alias	Specify an alias for the Fibre Channel port. The alias must consist of 1 to 20 characters from any of the following groups: • Letters: A-Z, a-z • Numbers: 0-9 • Special characters: Hyphen (-), underscore (_)
View initiators	View a list of all Fibre Channel initiators currently logged into the port.
Edit port binding	Modify the port binding for the port. Port binding allows you to restrict which initiators are allowed to connect to the port. For more information, see Fibre Channel Port Binding.

Fibre Channel Port Status

Status	Description
Connected	The port has an active network connection.
Disconnected	The port does not have an active network connection.

Fibre Channel Port Binding

Port binding is a Fibre Channel security method that enables you to restrict which initiator WWPNs are allowed to connect through a Fibre Channel port. It is similar to iSCSI target authorization.

Tip
By default, port binding is disabled on all Fibre Channel ports.

Configuring Fibre Channel Port Binding

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Ports** .
2. Select a Fibre Channel port.
3. Click **Action**, and then select **Edit Port Binding**.
   The **Fibre Channel Port Binding** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	**a.** Select one or more initiator WWPNs in the WWPN list. **b.** Click **Add**.
Add WWPNs as text	**a.** Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` **b.** Click **Add**.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
6. Click **OK**.

FC Storage

The **FC Storage** screen displays the LUN and Fibre Channel port group mappings.

Fibre Channel LUN Masking

LUN masking is a security feature that enables you to make a LUN visible to some Fibre Channel initiators and invisible to other initiators.

Configuring Fibre Channel LUN Masking

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC Storage** .
2. Select a LUN.

Important
The LUN must be disabled.

3. Click **LUN Masking**.
   The **LUN Masking** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	**a.** Select one or more initiator WWPNs in the WWPN list. **b.** Click **Add**.
Add WWPNs as text	**a.** Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX` **b.** Click **Add**.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
   When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
6. Select **Enable LUN**.
   If selected, QuTS hero will enable the LUN after mapping it to the target.
7. Click **OK**.

Fibre Channel LUN Actions

LUN Action	Description
Edit LUN Mapping	Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: • Mapping a LUN to a Fibre Channel Port Group • Mapping a LUN to an iSCSI Target
Edit LUN Masking	LUN masking is an authorization method that makes a Logical Unit Number (LUN) visible to some initiators and invisible to other initiators. For details, see Configuring Fibre Channel LUN Masking.
Show in Storage & Snapshots	Manage the LUN at **Storage & Snapshots** > **Storage** > **Storage/Snapshots**
Modify	Edit the LUN settings.
Enable	Enable the LUN if it is currently disabled.
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.
Delete	Delete the LUN and all data stored on it. **Important** This action is only available if the LUN is unmapped.
LUN Import/Export	Export the LUN to another server, a local NAS folder, or an external storage device. For details, see Creating a LUN Export Job.

Fibre Channel LUN Status

Status	Description
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.

FC WWPN Aliases

On the **FC WWPN Aliases** screen, you can view, edit, and add WWPNs and WWPN aliases. A WWPN (World Wide Port Name) is a unique identifier for Fibre Channel ports. A WWPN alias is a unique human-readable name for a Fibre Channel port that makes it easier to identify it.

Adding WWPNs

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
2. Click **Add**.
   The **Add WWPN** window appears.
3. Add one or more WWPNs to the list of known WWPNs using any of the following methods.

Method	Steps
Add WWPNs from logged-in Fibre Channel initiators.	Select **Add WWPNs from all logged-in FC initiators.**

Method	Steps
Add WWPNs as text	Specify one WWPN per line using any of the following formats: • `XXXXXXXXXXXXXXXX` • `XX:XX:XX:XX:XX:XX:XX:XX`

4. Click **Add**.

Configuring a WWPN Alias

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
2. Locate a WWPN.
3. Under **Alias**, specify an alias for the WWPN.
   The alias must consist of 1 to 20 characters from any of the following groups:
   - Letters: A-Z, a-z
   - Numbers: 0-9
   - Special Characters: Underscore (_), hyphen (-)
4. Click **Save**.

Removing a WWPN Alias

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
2. Locate a WWPN.
3. Clear the **Alias** field.
4. Click **Save**.

Exporting a List of WWPN Aliases

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .
2. Click **Export**.
   The file browser window opens.
3. In the file browser window, navigate to the folder where you want to save the file.
4. Specify a filename.
5. Click **Save**.

The list of WWPN aliases is saved to your local computer as a CSV file, in the format:

- Field 1: WWPN
- Field 2: Alias

```
11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2
```

Example CSV Output

Importing a List of WWPN Aliases

You can import a list of WWPNs and aliases from a CSV file in the following format:

- Field 1: WWPN
- Field 2: Alias

```
11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2
```

Example CSV File

Important

- Identical aliases will be overwritten from the CSV file.
- Lines not formatted correctly will be ignored.

1. Go to **iSCSI & Fibre Channel** > **Fibre Channel** > **FC WWPN Aliases** .

2. Click **Import**.
   The file browser window opens.
3. Locate and open the CSV file.

LUN Import/Export

With LUN Import/Export, you can back up a LUN as an image file to an SMB or NFS file server, local NAS folder, or external storage device. You can then import the LUN image file and restore the LUN on any QNAP NAS.

Creating a LUN Export Job

1. Go to **iSCSI & Fibre Channel** > **LUN Import/Export** .
2. Click **Create a Job**.
   The **Create LUN Export Job** windows opens.
3. Select **Export a LUN**.
4. Select a LUN.
5. Optional: Specify a job name.
   The name must consist of 1 to 55 characters from any of the following groups:
   - Letters: A to Z, a to z
   - Numbers: 0 to 9
   - Special characters: Underscore (_)
6. Click **Next**.
7. Select the destination folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	• IP address or host name • NFS folder or path
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	• IP address or host name • Username • Password • CIFS/SMB folder or path
Local Host	Local NAS shared folder or connected external storage device	• NAS shared folder or external device • Sub-folder

8. Click **Next**.
9. Optional: Specify a LUN image name.
   - The name must consist of 1 to 64 characters from any of the following groups:
     - Letters: A to Z, a to z

- Numbers: 0 to 9
- Special characters: Underscore (_), hyphen (-), space ( )

- The name cannot begin or end with a space.

10. Optional: Select **Use Compression** to compress the image file.
    When enabled, the image file will be smaller but exporting will take longer and will use more processor resources.
11. Select when the job will run.

Option	Description
Now	Run the job immediately after the job has been created. After this first run, the job will only run when manually started.
• Hourly • Daily • Weekly • Monthly	Run the job periodically according to the specified schedule.

12. Click **Next**.
13. Click **Apply**.

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 **Create a Job**.
   The **Create LUN Export Job** windows opens.
3. Select **Import a LUN**.
4. Optional: Specify a job name.
   The name must consist of 1 to 55 characters from any of the following groups:
   - Letters: A to Z, a to z
   - Numbers: 0 to 9
   - Special characters: Underscore (_)
5. Click **Next**.
6. Select the source folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	• IP address or host name • NFS folder or path

Option	Description	Required Information
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	• IP address or host name • Username • Password • CIFS/SMB folder or path
Local Host	Local NAS shared folder or connected external storage device	NAS shared folder or external device

7. Click **Next**.
8. Select the LUN image file.
9. Click **Next**.
10. Specify the import destination.

Option	Description	Required Information
Overwrite existing LUN	Import the image file data to an existing LUN. **Warning** All existing data on the LUN will be overwritten.	An existing LUN.
Create a new LUN	Import the image file as a new LUN.	• LUN name • LUN location. This will be a storage pool.

11. Click **Next**.
12. Click **Apply**.

QuTS hero creates the job, and then immediately runs it.

LUN Import/Export Job Actions

Action	Description
Edit	Edit the job.
Delete	Delete the job.
Start	Start the job.
Stop	Stop a running job.
View Logs	View the job's status, properties, details of its last run, and event logs.

LUN Import/Export Job Status

Action	Description
--	The job has not run yet.
Initializing	The job is preparing to run.

Action	Description
Processing	The job is running. The job's progress is displayed a percentage 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.

8. 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.

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.

Setting	Description
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.

Section	Description
Test Result	View the test results as a graph. Choose from the following views: • IOPS / Time • IOPS / Data Written • Data Written / Time **Tip** Use these graphs to compare what effect different amounts of over-provisioning have on random write speeds (IOPS).
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.

9. Network & Virtual Switch

About Network & Virtual Switch

Network & Virtual Switch is a QuTS hero utility that centralizes the creation, configuration, and control of network connections. Network & Virtual Switch also manages physical network interfaces, virtual adapters, Wi-Fi, and Thunderbolt connections in addition to controlling DHCP, DDNS,and gateway services.

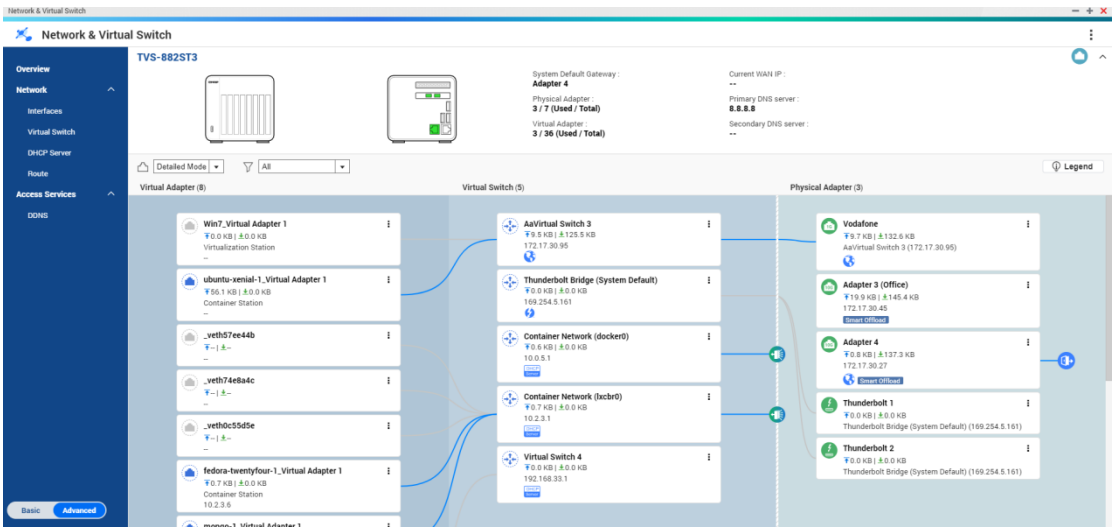
Basic and Advanced Mode

Network & Virtual Switch features two separate usage modes. Switch between these modes by clicking **Basic** or **Advanced** in the Network & Virtual Switch menu pane.

Mode	Description
Basic	This mode is well-suited for most users, and requires minimal configuration of network settings. • Virtual Switch functions are disabled. • Static Route functions are disabled.
Advanced	This mode is best-suited for power-users who need more control over the configuration of network settings. • Virtual Switch functions are enabled. • Static Route functions are enabled.

Overview

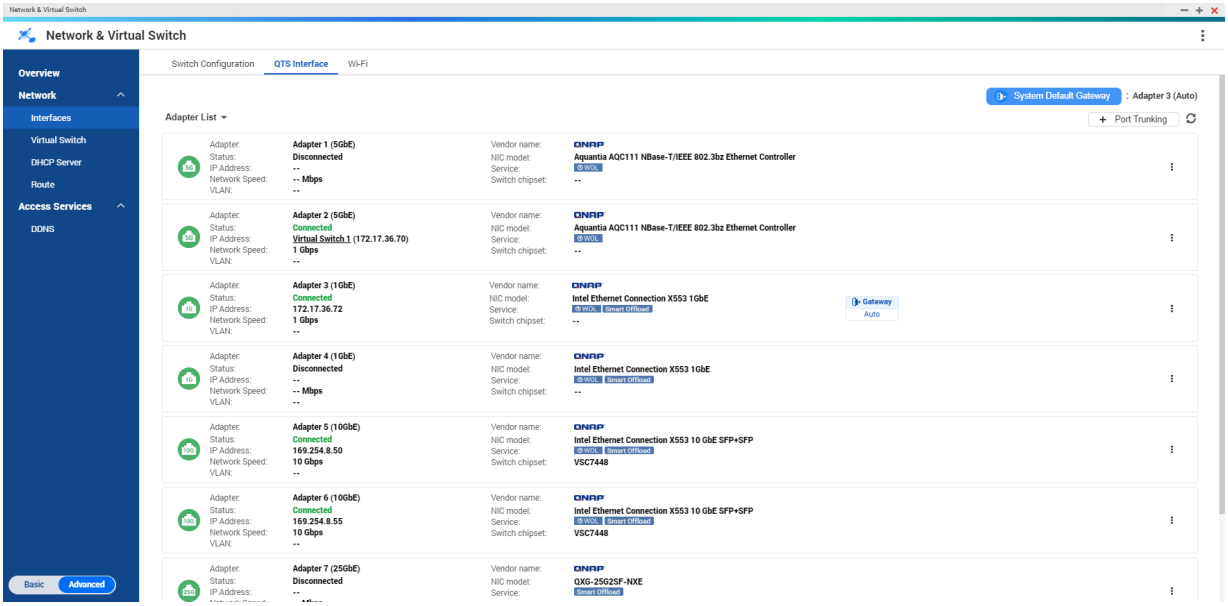
This screen provides a general overview of the network topology, IP address, status, and usage information for each device on the network.



Interfaces

This screen displays the physical adapter list as well as the physical adapter/SR-IOV topology when a Serial Root I/O Virtualization (SR-IOV) enabled network interface card (NIC) is connected to the device. The screen

provides access to basic network settings and allows the configuration of physical adapters. The Interface section allows you to configure settings related to IPv4, IPv6, DNS, port trunking, VLAN, Thunderbolt, USB QuickAccess, and Wi-Fi.



IP Address

Configuring IPv4 Settings

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Identify the adapter that you want to configure, then click ⋮ > **Configure** .
   The **Configure** window opens.
4. Configure the IPv4 settings.

Setting	Description
Obtain IP address settings automatically via DHCP	If the network supports DHCP, the adapter automatically obtains the IP address and network settings.
Use static IP address	Manually assign a static IP address. You must specify the following information: • Fixed IP Address • Subnet Mask • Default Gateway

Setting	Description
Jumbo Frame	Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. 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 NAS models support Jumbo Frames. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster.
Network Speed	Select the network transfer rate allowed by the network environment. **Tip** Selecting **Auto-negotiation** will automatically detect and set the transfer rate. **Important** The Network Speed field is automatically set to **Auto-negotiation** and hidden when configuring 10GbE & 40GbE adapters.

5. Click **Apply**.

Configuring IPv6 Settings

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Identify the adapter that you want to configure and then click > **Configure** .
   The **Configure** window opens.
4. Go to the **IPv6** tab.
5. Configure the IPv6 settings.

Setting	Description
Disable	Do not assign an IPv6 address.

Setting	Description
IPv6 Auto-Configuration (Stateful)	The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server. **Important** This option requires an available DHCPv6-enabled server on the network.
IPv6 Auto-Configuration (Stateless)	The adapter automatically acquires an IPv6 address and DNS settings from the router. **Important** This option requires an available IPv6 RA(router advertisement)-enabled router on the network.
Use static IP address	Manually assign a static IP address to the adapter. You must specify the following information: • Fixed IP Address • Prefix length **Tip** Obtain the prefix length information from your network administrator. • Default Gateway

6. Click **Apply**.

DNS

A Domain Name System (DNS) server translates a domain name into an IP address.

Configuring DNS Settings

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Identify the adapter that you want to configure, then click > **Configure** .
   The **Configure** window opens.
4. Go to the **DNS** tab.
5. Select one of the following options:

Setting	Description
Obtain DNS server address automatically	Automatically obtain the IP address using DHCP.

Setting	Description
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

6. Click **Apply**.

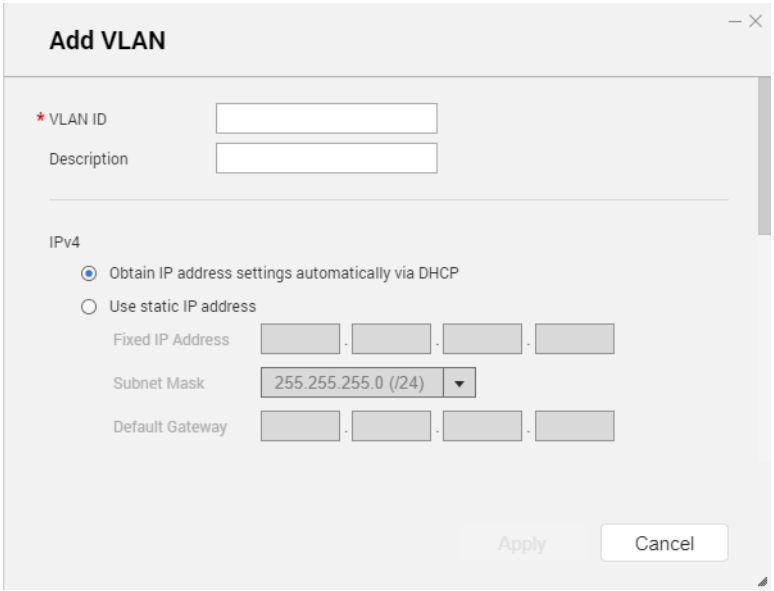
Virtual LANs (VLANs)

A virtual LAN (VLAN) 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.

Adding an Interface to a VLAN

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**.

Port Trunking

Port trunking combines two or more Ethernet interfaces for increased bandwidth, load balancing and fault tolerance (failover). Load balancing is a feature that distributes workloads evenly across multiple Ethernet interfaces for higher redundancy. Failover ensures that a network connection remains available even if a port fails.

Configuring Port Trunking

Important
Before configuring Port Trunking, ensure at least two network interfaces are connected to the same switch.

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Click **Port Trunking**.
The **Port Trunking** window opens.
4. Click **Add**.
The **Port Trunking (Add)** window opens.
5. Select two or more network interfaces to add to the trunking group.
6. Click **Next**.
7. Select a switch type.
8. Click **Next**.
9. Select a trunking mode.

Important
Some port trunking modes must be supported by your network switches. Selecting an unsupported mode may affect network performance or cause the network interface to freeze.

Mode	Description
Fault Tolerance (Failover)	
Active-Backup	All traffic is sent and received using the interface that was first added to the trunking group. If this primary interface becomes unavailable, the secondary interface will become active.
Broadcast	Transmits the same network packets to all the network interface cards.
Load balancing & Failover	
Balance-tlb	Incoming traffic is received by the current interface. If the interface fails, a slave interface takes over the MAC address of the failed interface. Outgoing traffic is distributed based on the current load for each interface relative to the interface's maximum speed.
Balance-alb	Similar to Balance-tlb, but offers additional load balancing for incoming IPv4 traffic.
Balance-rr	Transmits network packets sequentially to each network interface card in order to distribute the internet traffic among all the NICs.
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**.

System Default Gateway

The system default gateway serves as the network access point for the NAS. By default, all external network traffic will pass through the gateway. A network interface must be specified for the default gateway.

Configuring the System Default Gateway

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Click **System Default Gateway**.
   The **System Default Gateway** window opens.
4. Configure the system default gateway.

Setting	Description
Auto-select system default gateway	QuTS hero automatically detects all adapter, virtual switch, PPPoE, and VPN connections that can be used to connect to the internet. It selects one of these connections and then sets it as the default gateway.
Select the system default gateway	Manually assign an adapter to serve as the system default gateway. Optionally, set a backup failover gateway. The failover default gateway field is only available when multiple interfaces are connected. **Tip** When assigning a PPPoE or VPN connection as the default gateway, ensure a stable physical connection is also set as the failover default gateway.

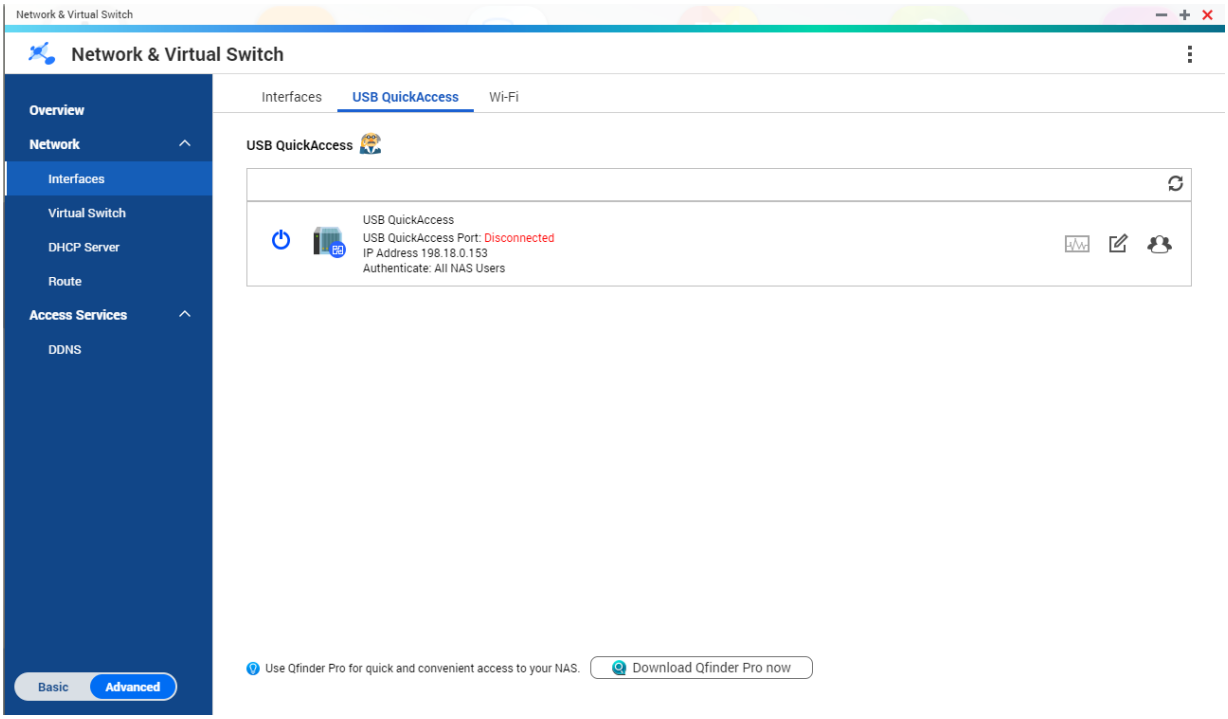
5. Optional: Disable the NCSI service.

Tip
The QuTS hero Network Connectivity Status Indicator (NCSI) periodically performs tests to check the speed and status of NAS network connections.

6. Click **Apply**.

USB QuickAccess

This screen controls the configuration and management of USB QuickAccess services on the NAS. USB QuickAccess allows a computer to connect to the NAS using a USB cable and the Common Internet File System (CIFS).



Tip

- USB QuickAccess is only available on certain models.
- It is not possible to configure, delete, or disable DHCP servers created with USB QuickAccess.

Enabling USB QuickAccess

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Go to the **USB QuickAccess** tab.
4. Click .

Configuring the USB QuickAccess IP address

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Go to the **USB Quick Access** tab.
4. Click .
   The **Configure** window opens.
5. Enter a static IP Address.
6. Click **Apply**.

Configuring USB QuickAccess Authentication

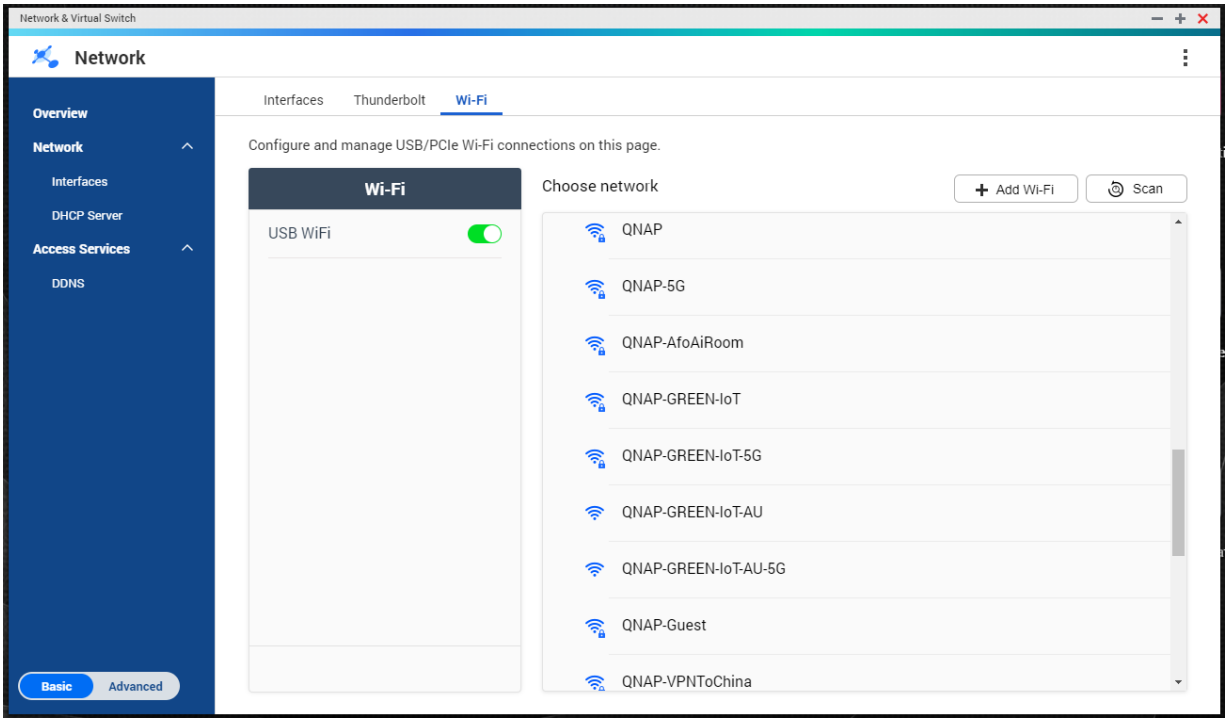
1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Go to the **USB Quick Access** tab.
4. Click .
   The **Configuration** window opens.
5. Select an authentication method:

Authentication Method	Description
All NAS Users	A QuTS hero username and password is required to access files.
Everyone	No username or password is required to access files.
Selected Users/Groups	Administrators can grant access to specific 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**.

Wi-Fi

This screen controls the configuration and management of Wi-Fi connections accessible from the NAS.



Important

- A USB or PCIe Wi-Fi device must be installed to access these features.
  - For a list of compatible USB Wi-Fi dongles, visit http://www.qnap.com/compatibility, then select **Search by Devices** > **USB Wi-Fi** .
  - For a list of compatible PCIe Wi-Fi cards, visit http://www.qnap.com/compatibility, then select **Search by Devices** > **Expansion Card** > **QNAP** .
- 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.

Enabling Wi-Fi

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Click .

Connecting to a Wireless Network

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .

3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible networks.
5. Select a wireless network from the list.

Icon	Description
	The Wi-Fi network requires a password.
	Connect to a Wi-Fi network without a password.
	• The Wi-Fi connection cannot access the internet. • The Wi-Fi connection requires an additional login. **Tip** QuTS hero does not support networks that require an additional login.

The settings panel expands.

6. Click **Connect**.
7. Optional: Configure connection settings.

Setting	Description
Password	Enter the password provided by the network administrator. **Tip** Click to make the password visible.
Connect automatically	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

8. Click **Apply**

Connecting to a Captive-Portal-Enabled Wireless Network Using Browser Station

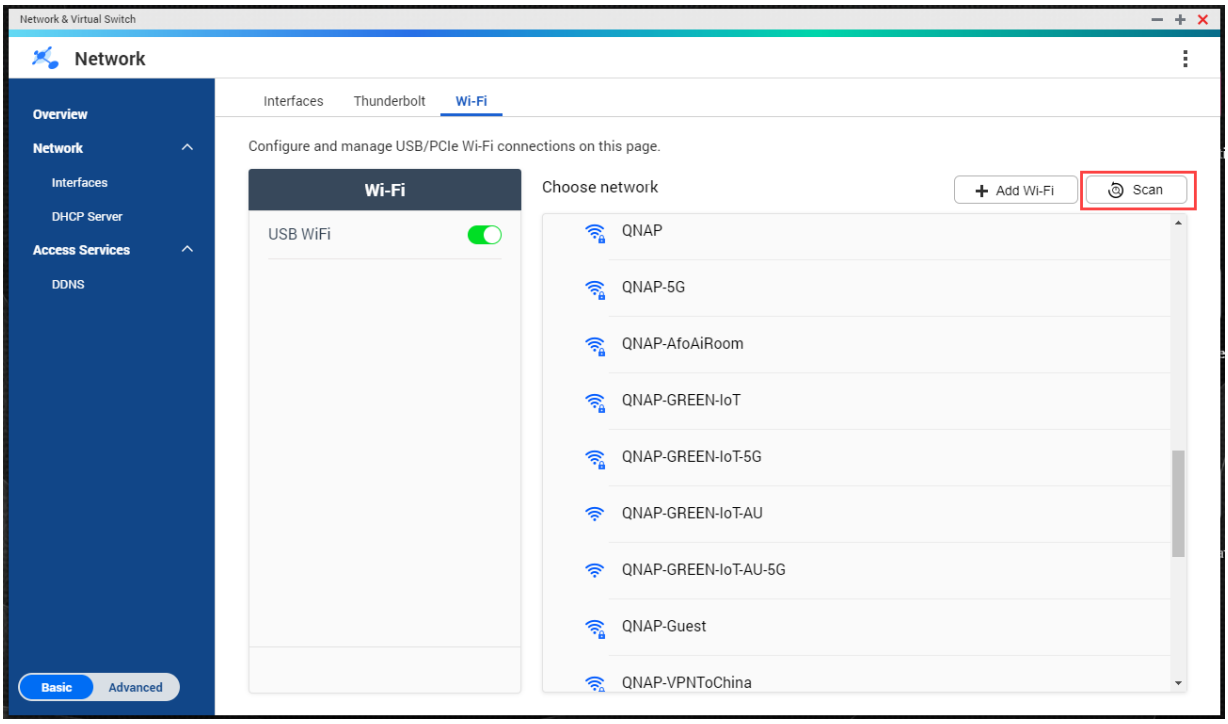
Captive portal allows organizations to easily share their network environment with customers, employees, and other guests.

QuTS hero supports the captive portal function that connects to the internet through an access point in the wireless network.

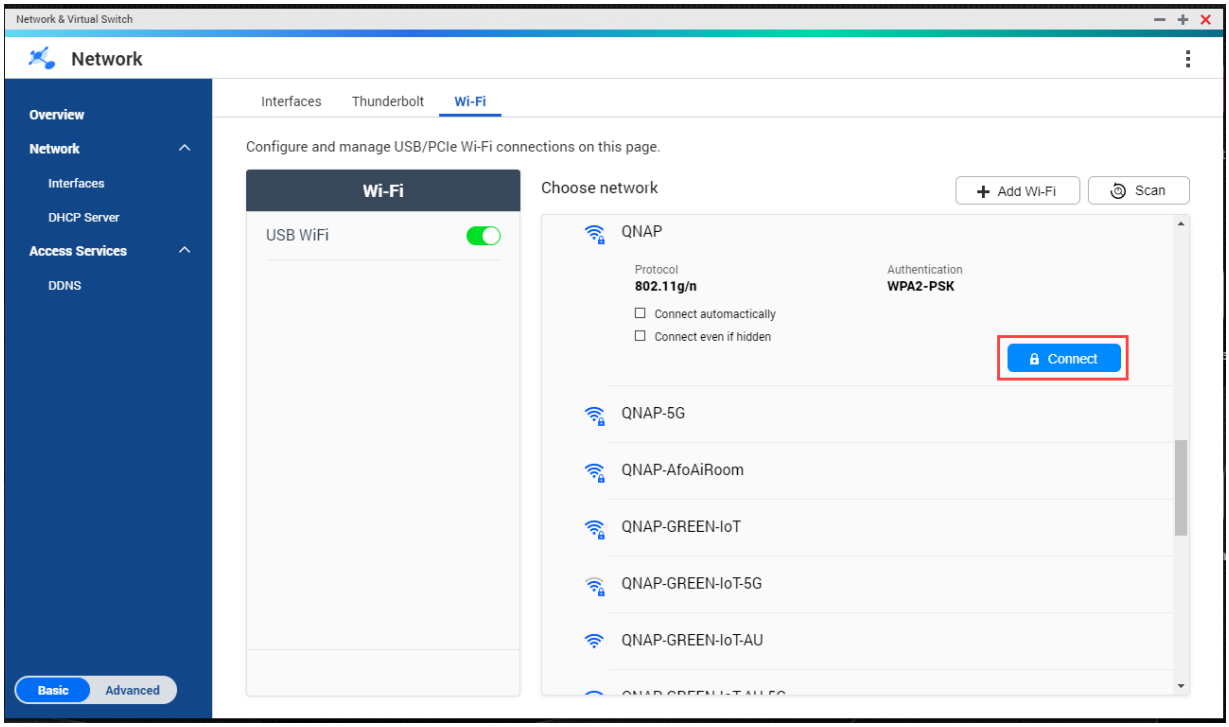
Note
Download and install Browser Station from App Center to access the captive portal functions.
Alternatively, QNAP recommends installing Qfinder Pro(6.9.2 or later) to utilize the captive portal function on a wireless network.
For details, see Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro.

1. Go to **Control Panel** > **Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.

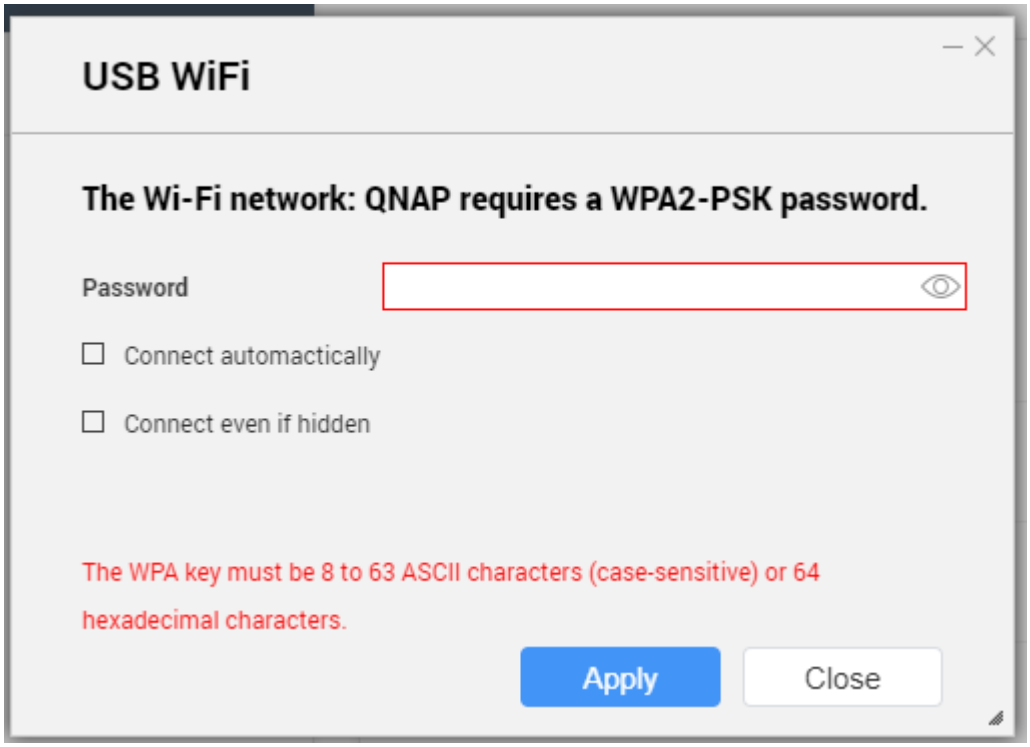
2. Go to **Network** > **Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible wireless networks enabled with captive portal.



5. Select the captive-portal-enabled wireless network from the list.
   The settings panel expands.
6. Click **Connect**.

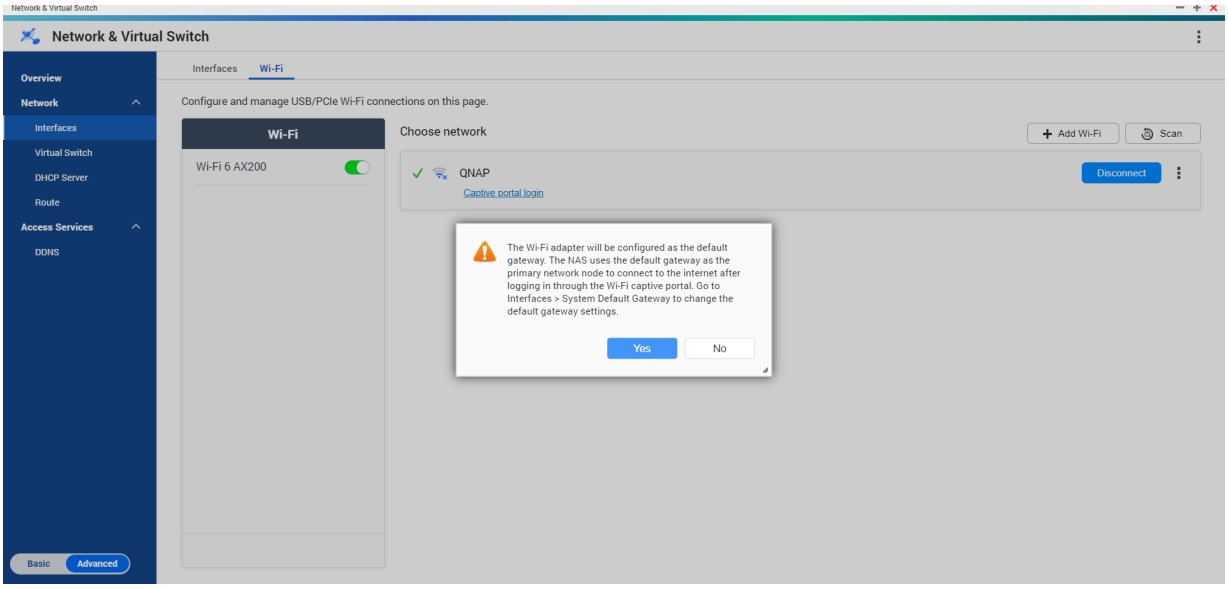


7. Optional: Configure connection settings.

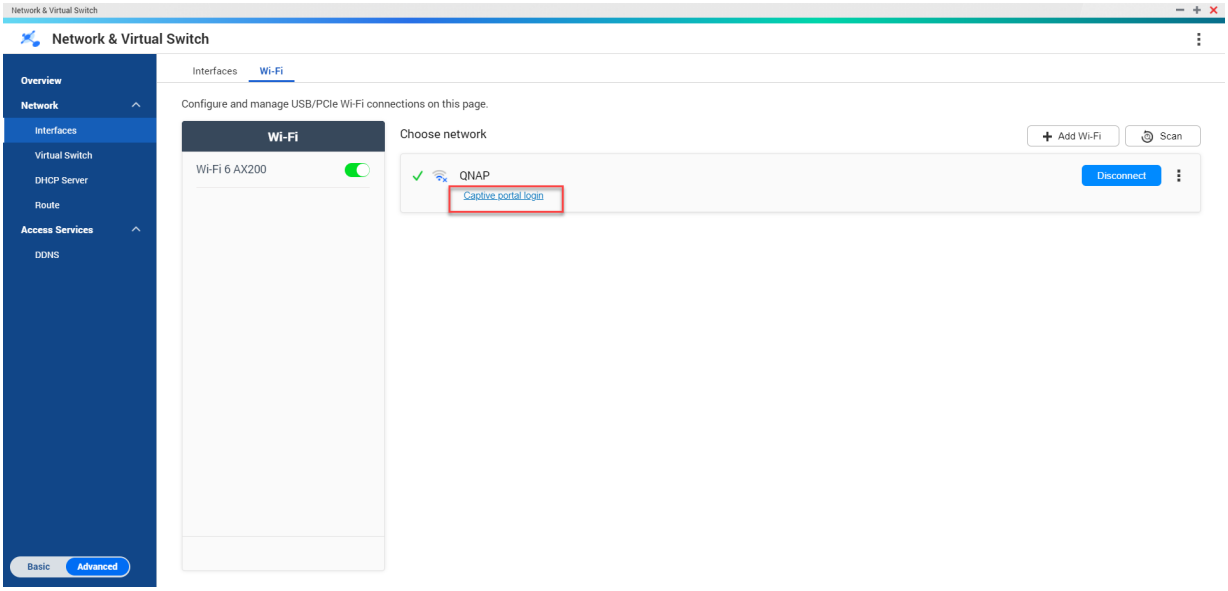


For configuration details and wireless icon descriptions, see Connecting to a Wireless Network.

8. Click **Apply**.
A pop-up 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.

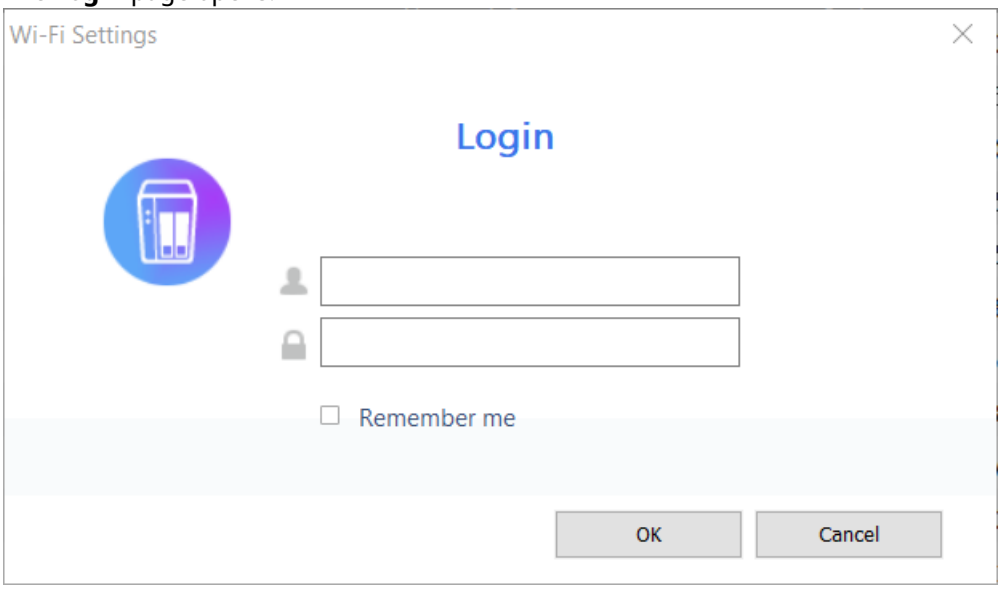
12. Enter the username and password to connect to the wireless network.

Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro

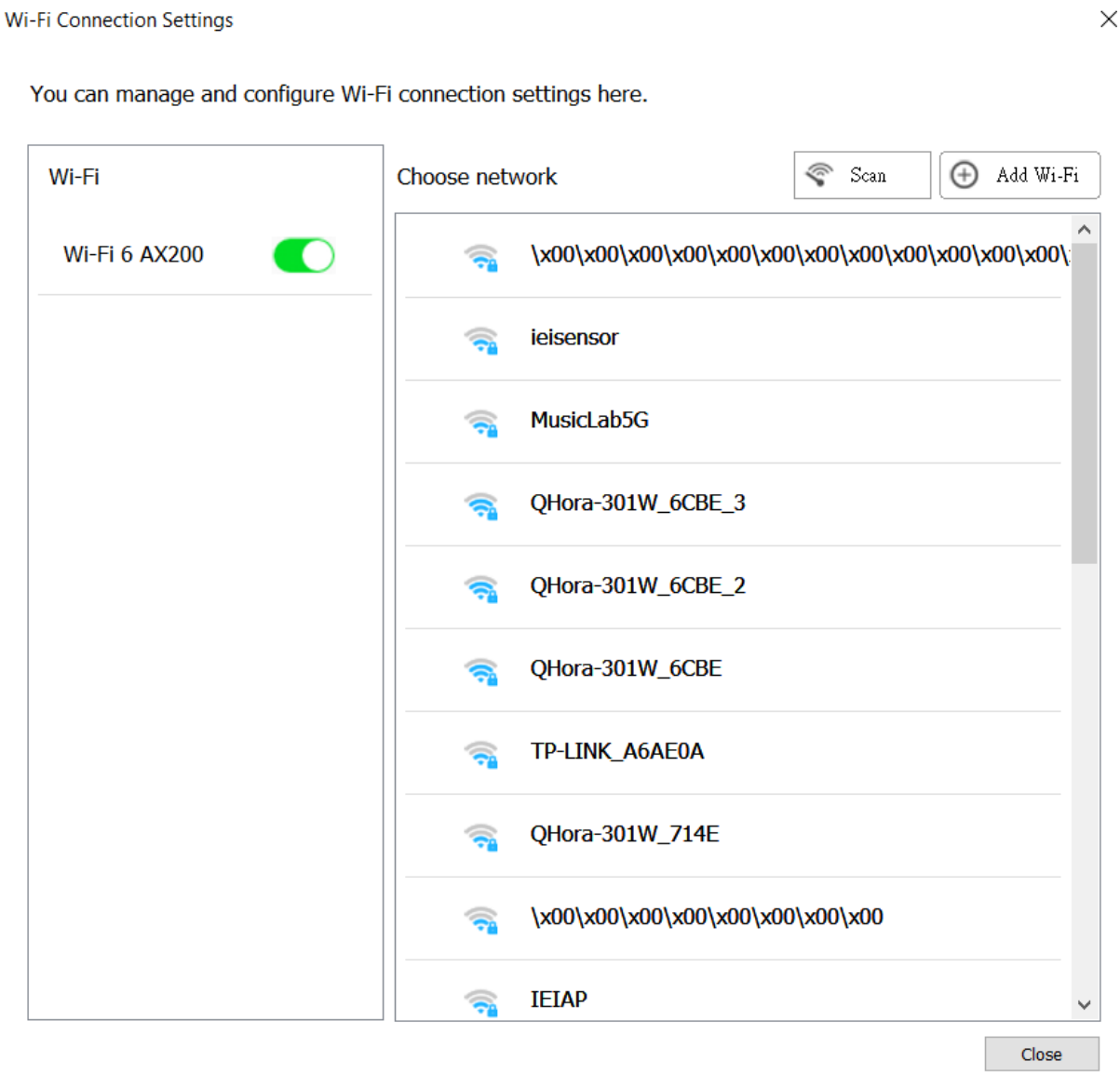
Note
QNAP recommends installing Qfinder Pro (Windows 6.9.2 or later and MacOS/Linux 7.3.2 or later) to utilize the captive portal function on a wireless network.

Important
Connect the NAS directly to the PC using an ethernet cable in order to connect to a wireless network enabled with captive portal.

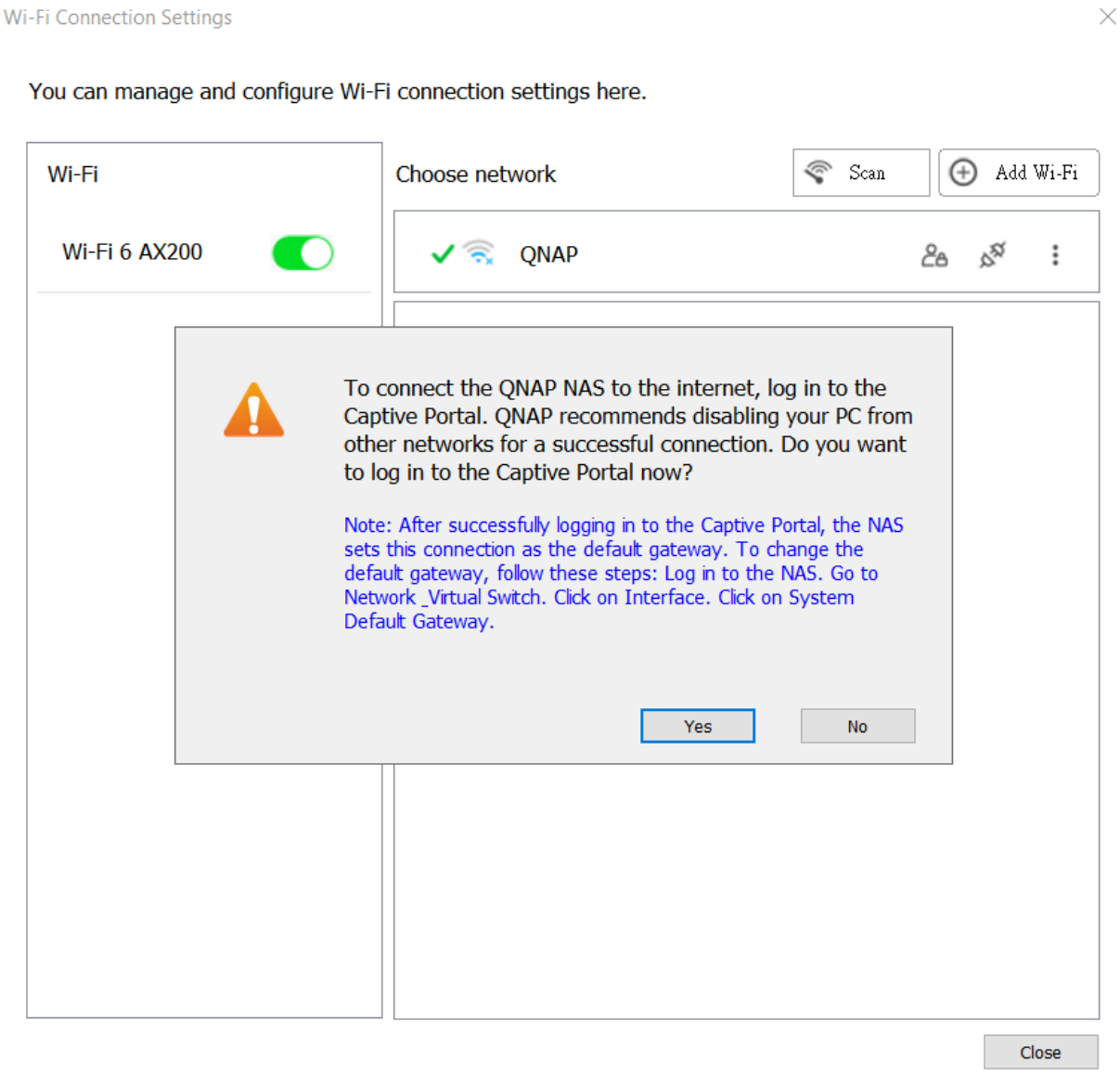
1. Open Qfinder Pro.
2. Locate the NAS in the list and click the unconfigured Wi-Fi icon located under the Status table header.
3. Optional: Alternatively, select the NAS and go to **Settings** > **Wi-Fi Settings** .
   The **Login** page opens.



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 pop-up 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.

Adding a Wireless Network

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Interfaces** .
3. Go to the **Wi-Fi** tab.

4. Click **Add Wi-Fi**.
   The **Connect to a Wi-Fi network** window opens.

5. Configure connection settings.

Setting	Description
Network Name	Enter the name of the wireless network.
Security Type	Select the encryption used by the wireless network. • **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.
Password	Enter the password provided by the network administrator. **Tip** Click to make the password visible.
Automatically connect when the	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

6. Optional: Configure WPA- & WPA2 Enterprise settings.

Setting	Description
Authentication	Authentication is specific to WPA- and WPA2- Enterprise encryption. You can select a method based on the authentication supported by your device. • **Protected EAP (PEAP)**: Protected Extensible Authentication Protocol (PEAP) provides a more secure authentication to 802.11 WLANs. • **EAP-TTLS**: EAP Tunneled Transport Layer Security (EAP-TTLS) supports legacy authentication mechanisms.
Certificate Authority (CA) File	A data file that contains identification credentials to help authenticate the WPA-WPA2 public key ownership. **Note** Select **CA file is not required** if you do not have access to a digital certificate.

Setting	Description
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.

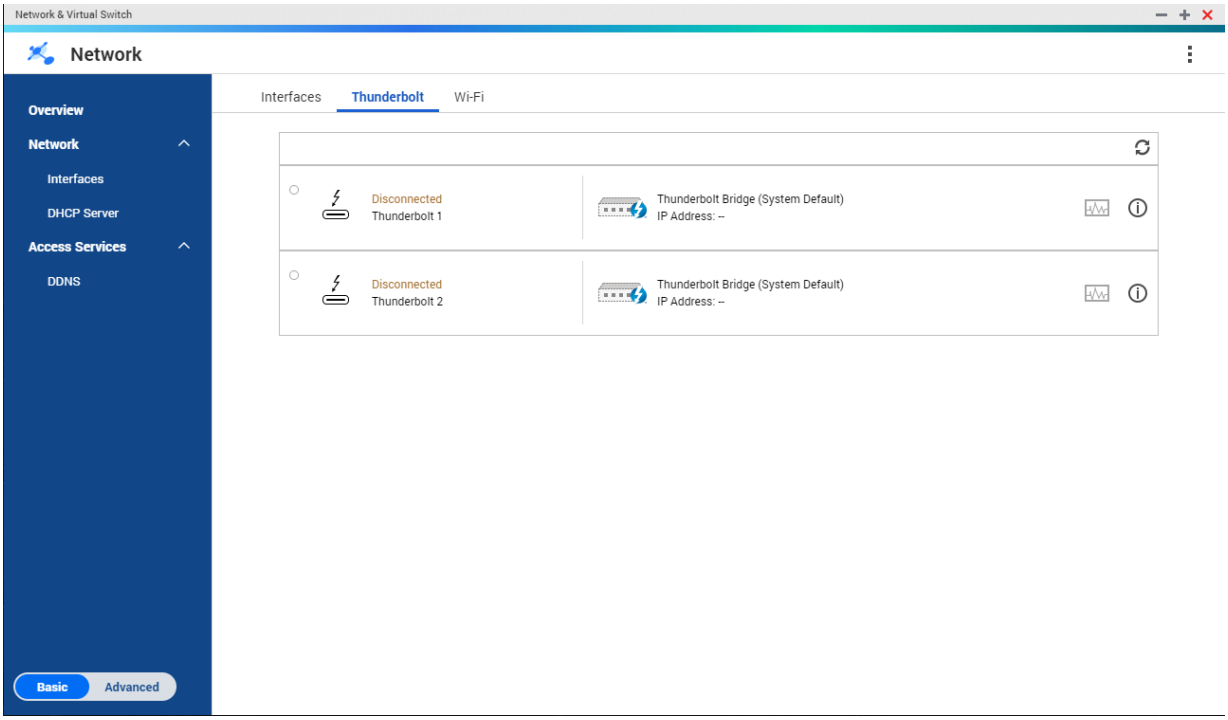
7. Click **Connect**.

Connection Messages

Message	Description
Connected	The NAS is currently connected to the Wi-Fi network.
Connecting	The NAS is trying to connect to the Wi-Fi network.
Out of range or hidden SSID	The wireless signal is not available or the SSID is not being broadcast.
Failed to get IP	The NAS is connected to the Wi-Fi network but could not get an IP address from the DHCP server. Check the router settings.
Association failed	The NAS cannot connect to the Wi-Fi network. Check the router settings.
Incorrect key	The entered password is incorrect.
Auto connect	Automatically connect to the Wi-Fi network. This is not supported if the SSID of the Wi-Fi network is hidden.

Thunderbolt

This screen displays port and connection information related to any Thunderbolt interfaces on the NAS.



Thunderbolt to Ethernet (T2E)

Thunderbolt to Ethernet functionality allows the Thunderbolt port to act as an Ethernet interface.

Tip
QNAP recommends using Qfinder Pro when configuring Thunderbolt to Ethernet.

Important
Due to Thunderbolt driver issues, T2E connections using Thunderbolt 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.

Tip
Qfinder Pro automatically configures the /etc/sysctl.conf settings file on macOS.

1. Open **Qfinder Pro**.
2. Locate the NAS using **Qfinder Pro**.
3. Click the Thunderbolt icon.
   The T2E window opens.
4. Select **Enable T2E**.
5. Click **Apply**.

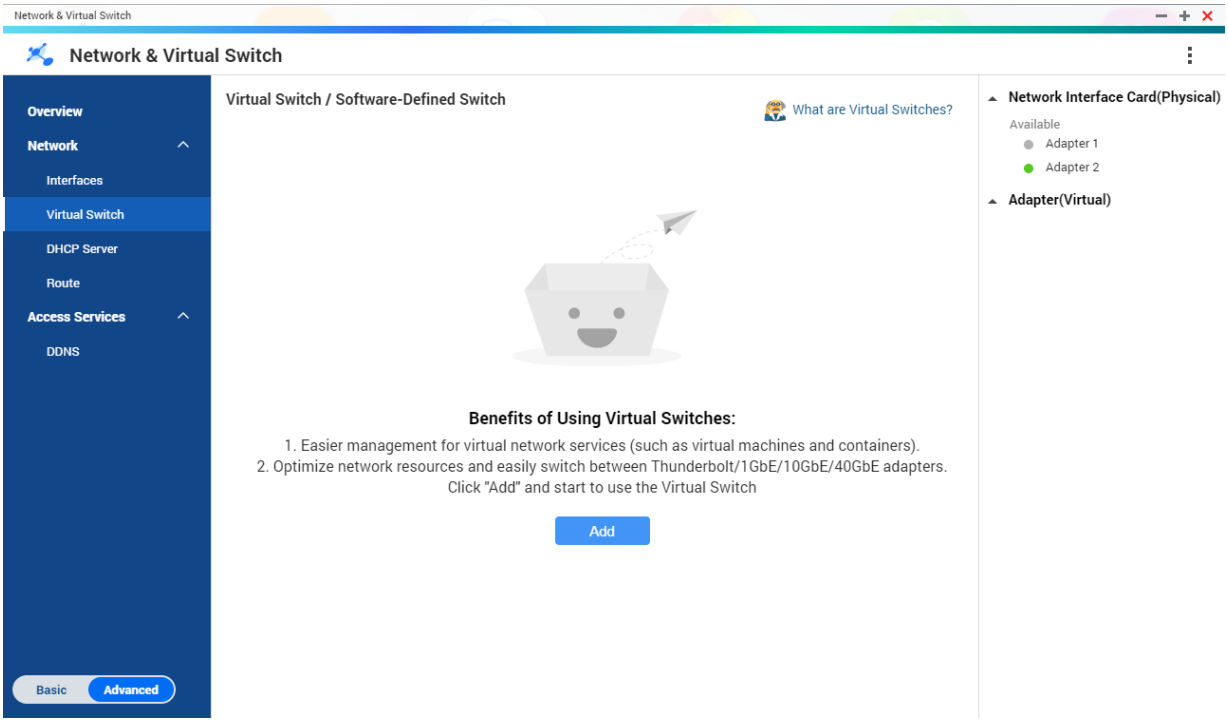
Enabling T2E on macOS

1. Open the Terminal.
2. Run the command.

Command	Notes
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.

Virtual Switches

This screen controls the configuration and management of virtual switches running on the NAS. Virtual Switches allow physical interfaces and virtual adapters to communicate with each other.



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.

Mode	Description
Software-Defined Switch	This mode is suited for power-users who need to simulate an L2 physical switch. **Important** Packet forwarding rates are limited when using this mode.

Tip
To access this page, Network & Virtual Switch must be operating in Advanced Mode.

Creating a Virtual Switch in Basic Mode

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Virtual Switch** .
3. Click **Add**.
   The **Create a Virtual Switch** window opens.
4. Select **Basic Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

Tip
Enabling this setting prevents bridge loops.

7. Click **Apply**.

Creating a Virtual Switch in Advanced Mode

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Virtual Switch** .
3. Click **Add**.
   The **Create a Virtual Switch** window opens.
4. Select **Advanced Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

Tip
Enabling this setting prevents bridge loops.

7. Click **Next**.
8. Configure the virtual switch IP address.

Address Type	Description
DHCP Client	Assigns a dynamic IP address to the virtual switch.
Static IP	Assigns a static IP address to the virtual switch. **Tip** Examine your network setup for guidance on how to best configure these settings.
Do not assign IP Addresses	Does not assign an IP address to the virtual switch after creation. **Tip** This setting should be used when creating a virtual switch for special purposes, such as when building an external or isolated network.

9. Click **Next**.
10. Configure the virtual switch services.
    a. Enable the NAT service.

Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- The IP address of the virtual switch cannot be in a reserved range that doesn't support forwarding:
  - 127.xxx.xxx.xxx
  - 169.254.xxx.xxx
  - 192.0.2.xxx
  - 198.51.100.xxx
  - 203.0.113.xxx

    b. Optional: Enable the DHCP Server.

Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- To avoid IP address conflicts, do not enable DHCP server if there is another DHCP server running on the local network.

Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.

Setting	Description
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.
WINS Server	Specify the WINS server IP address. **Tip** Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix. **Tip** The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server. **Tip** QuTS hero supports both PXE and remote booting of devices
Boot File	Specify location and file name of the TFTP server boot file. **Tip** QuTS hero supports both PXE and remote booting of devices

11. Click **Next**.
12. Configure the virtual switch IPv6 address.

Setting	Description
Disable	Do not assign an IPv6 address.
IPv6 Auto-Configuration (Stateful)	The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server. **Important** This option requires an available DHCPv6-enabled server on the network.
IPv6 Auto-Configuration (Stateless)	The adapter automatically acquires an IPv6 address and DNS settings from the router. **Important** This option requires an available IPv6 RA(router advertisement)-enabled router on the network.

Setting	Description
Use static IP address	Manually assign a static IP address. You must specify the following information: • Fixed IP Address • Prefix length **Tip** Obtain the prefix length information from your network administrator. • Default Gateway

13. Click **Next**.
14. Configure the DNS settings.

Setting	Description
Obtain DNS server address automatically	Automatically obtain the DNS server address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

15. Click **Next**.
16. Confirm the virtual switch settings.
17. Click **Apply**.

Creating a Virtual Switch in Software-defined Switch Mode

Important
To avoid bridge loops, please ensure any Ethernet cables are connected to the same switch before configuring a Software-defined Switch.

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Virtual Switch** .
3. Click **Add**.
   The **Create a Virtual Switch** window opens.
4. Select **Software-defined Switch Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

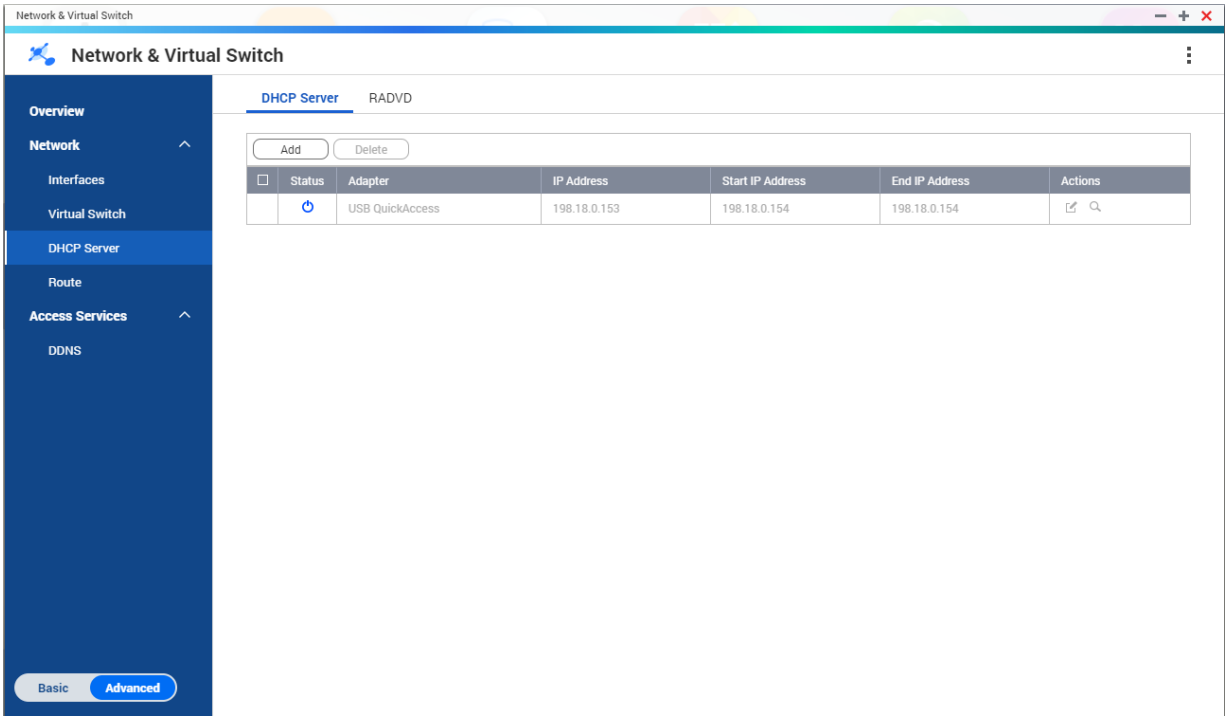
Tip
Enabling this setting prevents bridge loops.

7. Click **Apply**.

DHCP Server

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.

This screen controls the creation and management of DHCP servers. DHCP servers can assign IPv4 addresses to clients on the network, while RADVD servers assign IPv6 addresses.



Important
Do not create a new DHCP server if one already exists on the network. Enabling multiple DHCP servers on the same network can cause IP address conflicts or network access errors.

Creating a DHCP Server

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **DHCP Server** .
3. Click **Add**.
   The **DHCP Server** window opens.
4. Select an interface.
5. Click **Next**.

6. Select the network environment for the DHCP server.

Option	Description
Enable DHCP server on the current network.	• The adapter keeps the existing IP address and subnet mask. • The DHCP server shares the subnet mask with the adapter and is assigned the next available IP address.
Reassign an IP address to the adapter and enable a DHCP server on a new subnet.	• The adapter is assigned a new IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.
Enable DHCP server for another subnet.	• The adapter keeps the existing IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.

7. Click **Next**.
8. Configure a static IP address for the adapter.

Important
A static IP address must be configured when creating a DHCP server.

   a. Click **Yes**.
   b. Configure IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address. **Tip** Examine your network setup for guidance on how to best configure these settings.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Default Gateway	Specify the IP address of the default gateway for the adapter.
Jumbo Frame	Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QuTS hero supports the following Jumbo Frame sizes: • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes **Important** • Jumbo Frames are only supported by certain NAS models. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster. All connected network devices must enable Jumbo Frames and use the same MTU size.

Setting	Description
Network Speed	Specify the speed at which the adapter will operate. **Tip** **Auto-negotiation** will automatically detect and set the transfer rate.
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	Assign an IP address for the secondary DNS server. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Next**.

9. Configure DHCP settings.

Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.
WINS Server	Specify the WINS server IP address. **Tip** Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix. **Tip** The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server. **Tip** QuTS hero supports both PXE and remote booting of devices.

Setting	Description
Boot File	Specify location and file name of the TFTP server boot file. **Tip** QuTS hero supports both PXE and remote booting of devices.

10. Click **Apply**.

DHCP Clients

A DHCP client is a network device using DHCP service to obtain network cofiguration 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.

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

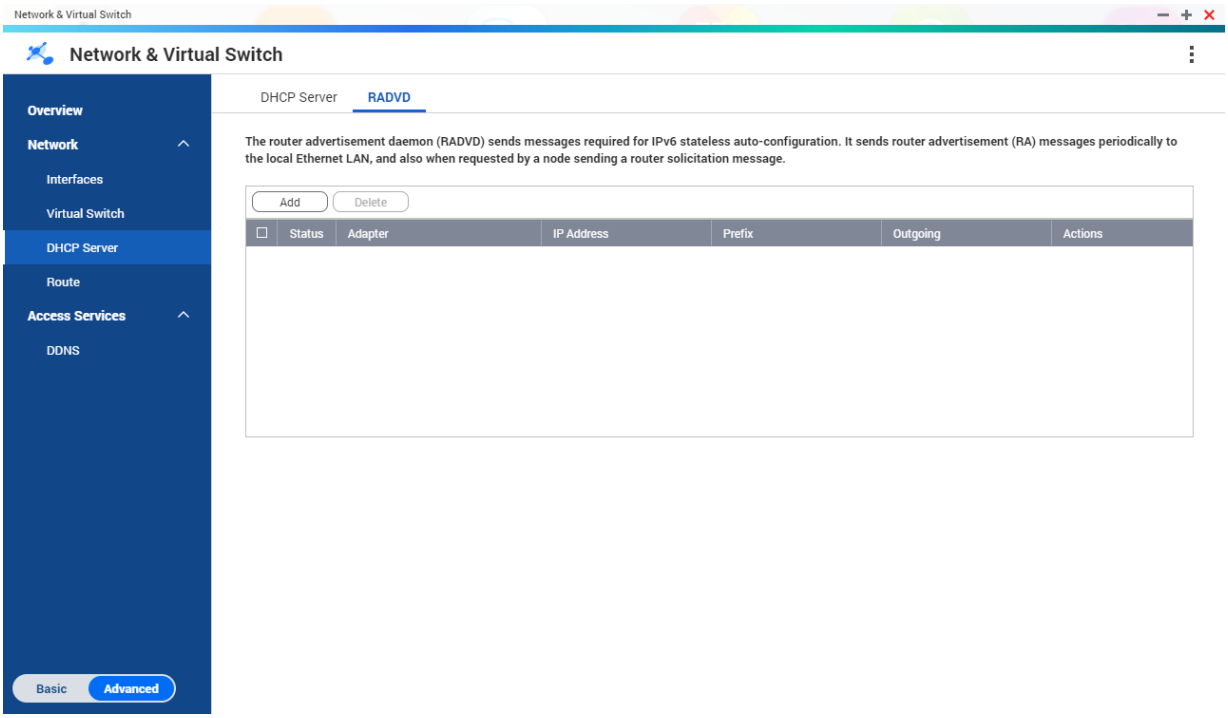
Virtual switches allow virtual machines to obtain IP-related configurations automatically from an external DHCP server. The virtual switch obtains the IP address from the DHCP server through the connected physical adapter on the device.

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 **Virtual Switch** > **Basic Mode/Advanced Mode** .

RADVD

This screen controls the creation and management of Router Advertisement Daemon (RADVD) servers. This service sends messages required for IPv6 stateless auto-configuration. This service periodically sends router advertisement (RA) messages to devices on the local network, and can also send a router solicitation messages when requested from a connected node.



Creating an RADVD Server

1. Go to **Control Panel** > **Network & File Services** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **DHCP Server** .
3. Go to the **RADVD** tab.
4. Click **Add**.
   The **RADVD - Outgoing Interface** window opens.
5. Select the outgoing interface.
6. Click **Next**.
7. Configure a static IP address for the adapter.

Important
A static IP address must be configured when creating a RADVD server.

   a. Click **Yes**.

   b. Optional: Configure Static IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address. **Tip** Examine your network setup for guidance on how to best configure these settings.

Setting	Description
Prefix Length	Specify the prefix length for the adapter. **Tip** Obtain the prefix and the prefix length information from your ISP.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	Assign an IP address for the secondary DNS server. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Next**.

8. Select a second adapter for the RADVD service interface.
9. Click **Next**.
10. Optional: Configure a static IP address for the second RADVD adapter.

Important
Creating an RADVD interface requires that the adapter use a static IP address. If the adapter already uses a static IP address, skip this step.

a. Click **Yes**.

b. Configure Static IP address settings.

Setting	Description
Fixed IP Address	Specify a fixed IP address. **Tip** Examine your network setup for guidance on how to best configure these settings.
Prefix Length	Specify the prefix length for the adapter. **Tip** Obtain the prefix and the prefix length information from your ISP.
Default Gateway	Specify the IP address of the default gateway for the adapter.
Primary DNS Server	Specify the DNS server address.
Secondary DNS server	Specify the DNS server address. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Click **Apply**.

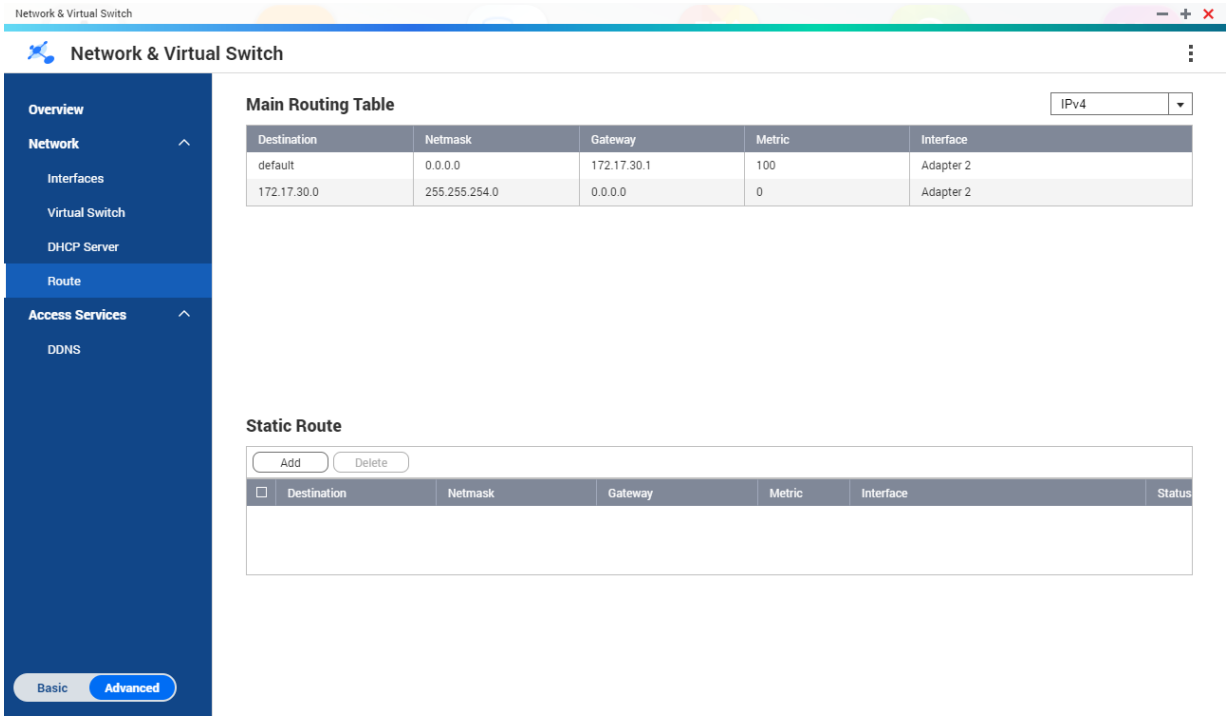
11. Configure the RADVD server settings.

Setting	Description
Prefix	Specify the routing prefix for the adapter. **Tip** Examine your network setup for guidance on how to best configure these settings.
Prefix Length	Specify the prefix length for the adapter. **Tip** Obtain the prefix and the prefix length information from your ISP.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Primary DNS Server	Specify the DNS server address.
Secondary DNS server	Specify the DNS server address. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

12. Click **Apply**.

Route

This screen controls the creation of static routes. Under normal circumstances, 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.



Creating a Static Route

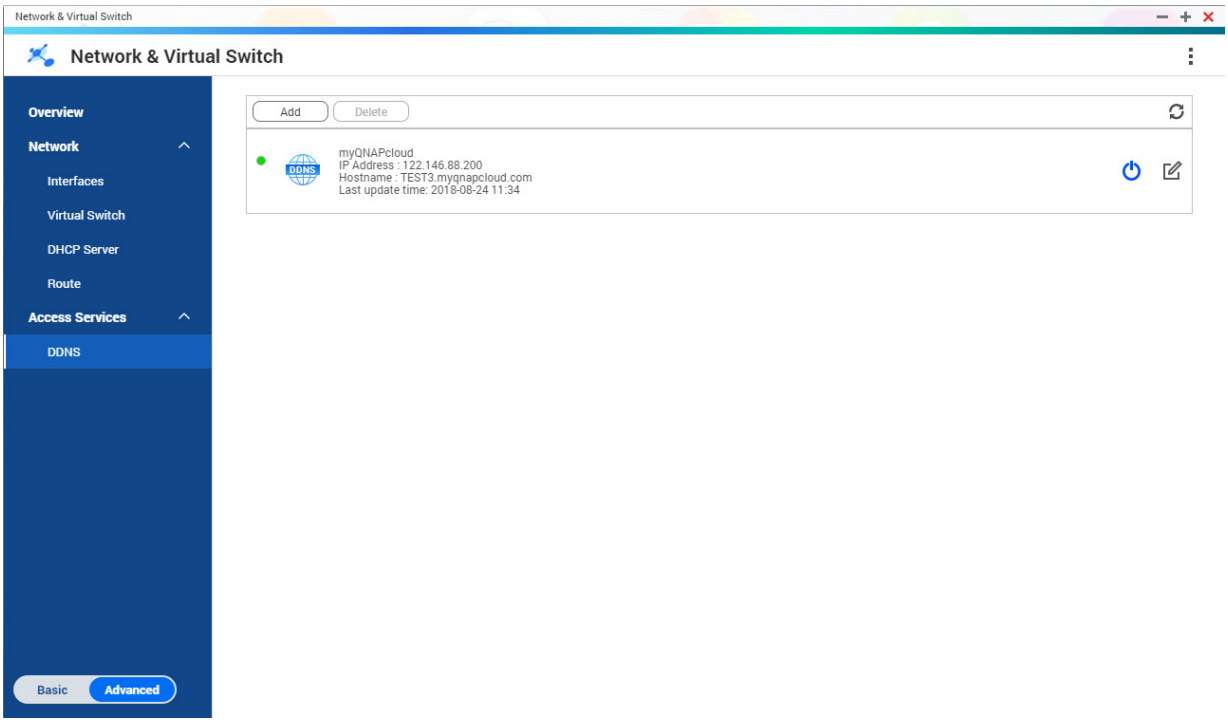
1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **Route** .
3. Click **Add**.
   The **Static Route (IPv4)** window opens.
4. Configure the IP address settings.

Setting	Description
Destination	Specify a static IP address where connections are routed to.
Netmask	Specify the IP address of the destination's netmask.
Gateway	Specify the IP address of the destination's gateway.
Metric	Specify the number of nodes that the route will pass through. **Note** Metrics are cost values used by routers to determine the best path to a destination network.
Interface	Select the interface that connections should be routed through.

5. Click **Apply**.

DDNS

This screen controls the management of Dynamic Domain Name System (DDNS) services. DDNS allows access to the NAS from the internet using a domain name rather than an IP address.



Adding a DDNS Service

1. Go to **Control Panel** > **Network & Virtual Switch** .
   The **Network & Virtual Switch** window opens.
2. Go to **Network** > **DDNS** .
3. Click **Add**.
   The **DDNS (Add)** window opens.
4. Configure the DDNS settings.

Setting	Description
Select DDNS server	Select the DDNS service provider.
Username	Specify the username for the DDNS service.
Password	Specify the password for the DDNS service.
Hostname	Specify the hostname or domain name for the DDNS service.
Check the External IP Address	Specify how often to update the DDNS record.

5. Click **Apply**.

10. 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)
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
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

Configuring 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 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 filesystem. 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 3 trap addresses.

4. Select the SNMP version that the NMS uses.

Option	User Action
SNMP V1/V2	Specify an SNMP community name that contains 1 to 64 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and the NAS. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.
SNMP V3	Specify the username, authentication protocol and password, and privacy protocol and password. **a.** Specify a username. **Note** The username should contain 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ **b.** Optional: Select **Use Authentication**. **1.** Specify the authentication protocol. **Tip** You can select either **HMAC-MD5** or **HMAC-SHA**. If you are unsure about this setting, QNAP recommends selecting **HMAC-SHA**. **2.** Specify an authentication password that contains 8 to 64 ASCII characters. **c.** Optional: Select **Use Privacy**. **1.** Specify a privacy password that contains 8 to 64 ASCII characters.

5. Click **Apply**.

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 1.3.6.1.4.1.24681.2.

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.

Configuring File Sharing Protocol Settings

File sharing protocols allows users to access shared resources on a server that supports the file sharing protocol of each client. Shared file access is implemented over local area network (LAN) service and implements automatic synchronization of folder information whenever a folder is changed on the server.

Configuring Samba (Microsoft Networking) Settings

Microsoft Networking refers to Samba, a network protocol that allows data to be accessed over a computer network and provides file and print services to Windows clients.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **Microsoft Networking** .
2. Select **Enable file service for Microsoft networking**.
3. Configure Microsoft networking settings.

Setting	User Action
Server description (Optional)	Specify a description that contains a maximum of 256 characters. The description should enable users to easily identify the NAS on a Microsoft network.
Workgroup	Specify a workgroup name that contains 1 to 15 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: ~ ! @ # $ ^ & ( ) - _ { } . '

4. Select an authentication method.

Option	Description
Standalone server	QuTS hero uses the local user account information for authentication.
AD domain member	QuTS hero uses Microsoft Active Directory (AD) for authentication.
LDAP domain authentication	QuTS hero uses an LDAP directory for authentication.

5. Configure the advanced settings.
   a. Click **Advanced Options**.
      The **Advanced Options** window opens.
   b. Configure the advanced settings.
   c. Configure any of the following settings.

Option	User Action
Enable WINS server	Select to run a WINS server on the NAS.
Use the specified WINS server	Select to specify a WINS server IP address that QuTS hero will use for name resolution.
Local master browser	Select to use the NAS as a local master browser. A local master browser is responsible for maintaining the list of devices in a specific workgroup on a Microsoft network. **Important** To use the NAS as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".
Allow only NTLMSSP authentication	Select to authenticate clients using only NT LAN Manager Security Support Provider. When this option is deselected, QuTS hero uses NT LAN Manager (NTLM).
Name resolve priority	Select a name service to use for name resolution. The default service is **DNS only**. If a WINS server is specified, **Try WINS then DNS** is selected by default.
Alternative login style	Select to change how usernames are structured when accessing FTP, AFP, or File Station services. After selecting this option, users can access NAS services using Domain\Username, instead of Domain+Username.
Automatically register in DNS	Select to register the NAS on the DNS server. If the NAS IP address changes, the NAS automatically updates the IP address on the DNS server. This option is only available if AD authentication is enabled.
Enable trusted domains	Select to join users from trusted AD domains. This option is only available if AD authentication is enabled.
Enable Asynchronous I/O	Select to improve the Samba performance using asynchronous I/O. Asynchronous I/O refers to the I/O behavior on the CIFS protocol layer. This is different from the synchronous I/O feature found in the shared folder settings, which only applies to specific shared folders on the file system level. **Tip** To prevent power interruption, use a UPS when asynchronous I/O is enabled.
Enable WS-Discovery to help SMB clients discover the NAS	Select to enable Web Services Dynamic Discovery (WS-Discovery). WS-Discovery makes the NAS visible in File Explorer on Windows 10 computers.
Highest SMB version	Select the highest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting. **Note** Selecting SMB3 will also include SMB 3.1 and SMB 3.1.1.

Option	User Action
Lowest SMB version	Select the lowest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting. **Note** Selecting SMB 3 will also include SMB 3.1 and SMB 3.1.1.
Enable kernel-mode SMB daemon	Select to increase read/write performance. **Important** Enabling this option disables SMB encryption for shared folders.
Allow Symbolic links within a shared folder	Select 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.
Allow Symbolic links between different shared folders	Select to allow symbolic links between shared folders. **Note** This setting requires **Allow Symbolic links within a shared folder** to be selected first.
Restrict anonymous users from accessing SMB shared folders	Select to enable user login before accessing SMB shared folders. **Note** This setting will be locked to **Enabled (strict)** if ABSE is enabled on any shared folder.
Veto files	Enable to hide files from users accessing the NAS via SMB. Files are hidden if their filename matches a pattern in the veto criteria file.
Veto criteria	Specify filename criteria for hiding files from SMB NAS users. **Note** This option is only available when **Veto files** is selected.

   d. Click **Apply**.
      The **Advanced Options** window closes.

6. Click **Apply**.

Network & File Services saves the Samba settings.

Configuring AFP (Apple Networking) Settings

The Apple Filing Protocol (AFP) is a file service protocol that allows data to be accessed from a macOS device and supports many unique macOS attributes that are not supported by other protocols.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **Apple Networking** .
2. Select **Enable AFP (Apple Filing Protocol)**.
3. Optional: Select **DHX2 authentication support**.

4. Click **Apply**.

Network & File Services saves the AFP settings.

Configuring NFS Service Settings

Network File System (NFS) is a file system protocol that allows data to be accessed over a computer network. Enabling the NFS service allows Linux and FreeBSD users to connect to the NAS.

The NFS service supports the following permissions in the NFS host access settings. You can apply these permissions to shared folders in **Control Panel** > **Privilege** > **Shared Folders** > **Edit Shared Folder Permissions** , and then selecting **NFS host access** as the permission type.

Permission	Status	Description
sync	Disabled	Disabling **sync** allows the NFS server to override the NFS protocol and reply to requests before any changes made by that request have been committed to stable storage. Using this option usually improves performance, but could result in an unclean server restart (e.g., a server crash), data loss, or corruption.
	Enabled	• **wdelay**: Causes the NFS server to delay writing to the disk to accommodate requests committed to stable storage. • **no wdelay**: The NFS server normally delays committing a write request to disc if it suspects another related write request is in progress or arriving soon. This allows multiple write requests to be committed to the disc with the one operation which can improve performance. **no wdelay** is available to turn off the delay behavior if an NFS server received mainly small unrelated requests. The default can be explicitly requested with the wdelay option.
secure	Disabled	Disabling **secure** requires that requests originate on TCP/IP ports above 1024.
	Enabled	Enabling **secure** requires that requests originate on TCP/IP ports between 1-1024.
Security	Enabled	The transparent file sharing system offered by NFS exposes the data to several security vulnerabilities. The security mechanism allows safe network transmission over trusted networks. NFS protocol provides the following security options to enable secure data transfer between the server and the client. • **sys**: sys or AUTH_SYS is the default unencrypted NFS version 3 security mechanism • **krb5**: Use Kerberos for authentication only. • **krb5i**: Use Kerberos for authentication, and include a hash with each transaction to ensure data integrity. Traffic can still be intercepted and examined, but modifications to the traffic are made apparent. • **krb5p**: Use Kerberos for authentication, and encrypt all traffic between the client and server. This authentication is the most secure mechanism but also incurs the most load.

Permission	Status	Description
Squash	Enabled	Remote root users can change any file on the shared file system and expose other users to executable Trojan-infected applications. The squash permission enables the NFS server to transfer the client root role and prevent possible security threats. • **Squash root users**: Maps the remote root user identity to a single anonymous identity and denies the user special access rights on the specified host. • **Squash all users**: Maps all the client requests to a single anonymous identity on the NFS server. • **Squash no users**: The default option does not transfer the client root role.

1. Go to **Control Panel** > **Network & File Services** > **Win/Mac/NFS/WebDAV** > **NFS Service** .
2. Enable NFS Service.
   a. Optional: Click **Enable NFS v2/v3 Service**.
   b. Optional: Click **Enable NFS v4 Service**.
3. Click **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. Click **Apply**.

Network & File Services saves the NFS service settings.

Configuring FTP Settings

The FTP service helps optimize FTP data transfer. To use the service, you must configure the settings and then connect the device to an FTP client such as FileZilla.

1. Go to **Control Panel** > **Network & File Services** > **FTP** > **FTP Service** .
2. Select **Enable FTP Service**.
3. Configure the followings settings.

Setting	User Action
Protocol type	Select at least one FTP type: • **FTP (standard)** • **FTP with SSL/TLS (explicit)**
Port number	Specify a port number between 1 and 65535
Unicode support	Specify whether you want to enable Unicode support for filenames
Enable anonymous	Select **Yes** to allow anonymous users to access files via FTP.
Connection	

Setting	User Action
Maximum number of all FTP connections	Specify a value between 2 and 1024
Maximum number of connections for a single account	Specify a value between 2 and 1024
Enable FTP transfer limitation	Enable this option to specify the maximum upload and download rate
Maximum upload rate (KB/s)	Select this option to specify the maximum upload rate of files over FTP. You must specify a value of at least 1.
Maximum download rate (KB/s)	Select this option to specify the maximum download rate of files over FTP. You must specify a value of at least 1. **Note** The maximum number of allowed connections for a single account must be lower than the maximum number of total allowed FTP connections.

4. Click **Apply**.

Configuring Advanced FTP Settings

1. Go to **Control Panel** > **Network & File Services** > **FTP** > **FTP Service** .
2. Select **Enable FTP Service**.
3. Go to **Advanced**.
4. Configure the following advanced FTP settings.

Setting	Description
Passive FTP Port Range	You can use the default port range (55536-56559) or specify a port range larger than 1023. When using this function, make sure you have opened the ports on your router or firewall.
Respond with external IP address for passive FTP connection request	Enable this function when a passive FTP connection is in use, the FTP server (NAS) is behind a router, and a remote computer cannot connect to the FTP server over the WAN. When this is enabled, the NAS replies with the specified IP address or automatically detects an external IP address so that the remote computer is able to connect to the FTP server.
Set root directory	After enabling this function and selecting a root directory, only that directory will be visible to FTP users. Otherwise, all of the shared folders will be visible.

5. Click **Apply**.

Enabling 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.

Network Recycle Bin Management

The Network Recycle Bin contains files deleted from the device through File Station, FTP settings, or by clients connected using Samba (Microsoft networking).

Configuring the Network Recycle Bin

1. Go to **Control Panel** > **Network & File Services** > **Network Recycle Bin** .
2. Select **Enable Network Recycle Bin**.
3. Optional: Configure the Network Recycle Bin settings.

Setting	Description
File retention time	Specify the number of days files are retained. The **Daily check time** controls when recycled files are checked against the retention time. **Tip** This field supports a maximum of 9999 days. The default is 180 days.

Setting	Description
Exclude these file extensions	Specify which file extensions are excluded from the Network Recycle Bin. **Important** File types are case insensitive and must be separated by a comma.

4. Click **Apply**.

Deleting All Files in the Network Recycle Bin

1. Go to **Control Panel** > **Network & File Services** > **Network Recycle Bin** .
2. Click **Empty All Network Recycle Bin**.
   A warning message appears.
3. Click **OK**.
   QuTS hero deletes all files from the Network Recycle Bin.

Restricting Access to the Network Recycle Bin

1. Go to **Control Panel** > **Privilege** > **Shared Folders** .
2. Identify a shared folder.
3. Under **Actions**, click .
   The **Edit Properties** window appears.
4. Select **Enable Network Recycle Bin**.
5. Select **Restrict the access to Recycle Bin to administrators only for now**.
6. Click **OK**.

11. myQNAPcloud

myQNAPcloud is a service that allows you to access, manage, and share files stored on your QNAP devices remotely through the internet.

Getting Started

1. Create a QNAP ID.
   For details, see Creating a QNAP ID With Email or Phone Number.
2. Register the device to myQNAPcloud.
   For details, see Registering a Device to myQNAPcloud.
3. Optional: Configure any of the following settings.

Settings	Description
Port forwarding	Port forwarding allows you to access your device on the internet through a UPnP router. For details, see Configuring UPnP Port Forwarding.
My DDNS	My DDNS allows you to specify a dedicated myQNAPcloud subdomain name that you can use to access your device on the internet. For details, see Configuring DDNS Settings
Published services	You can publish QNAP services on your device, such as the QNAP desktop and File Station, so they can be accessible on myQNAPcloud. For details, Configuring Published Services.
myQNAPcloud Link	myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to client device. For details, see Enabling myQNAPcloud Link.
Access controls	Access controls allow you to configure device access permissions for myQNAPcloud users. For details, see Configuring Device Access Controls.
SSL certificates	myQNAPcloud allows you to add SSL certificates to help secure your network communication. You can either download and install a myQNAPcloud or Let's Encrypt certificate. For details, see Installing an SSL Certificate.

Account Setup

Before using myQNAPcloud services, you must first create a QNAP ID and then configure required settings using your QNAP ID.

Creating a QNAP ID With Email or Phone Number

1. Go to https://account.qnap.com/.
   The **QNAP Account** login page displays.
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.

Registering a Device to myQNAPcloud

1. Log on to QuTS hero as administrator.
2. Go to **myQNAPcloud** > **Overview** .
3. Click **Get Started**.
   The **myQNAPcloud wizard** appears.
4. Click **Start**.
5. Specify your QNAP ID and password.
6. Click **Next**.
7. Specify a device name containing up to 30 alphanumeric characters.
   You may reuse an existing device name. The device currently using this name will be deregistered from myQNAPcloud.
8. Click **Next**.
9. Select the services you want to enable.

Service	Description
Auto Router Configuration	This allows you to configure port forwarding.
DDNS	This allows you to access your device on the internet using a dedicated address.
Published Services	This allows you to select which services you want to publish on the myQNAPcloud website.
myQNAPcloud Link	myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to client device. If you enable this option and your device does not have myQNAPcloud Link, myQNAPcloud Link will automatically be downloaded and installed after you click **Next**.

10. Select an access control option.

Option	Description
Public	All users can search for your device and view the published services on the myQNAPcloud website. They can also access your device with a SmartURL.

Option	Description
Private	Your device will not appear in the search results. Only you can access your device on the myQNAPcloud website.
Customized	Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL.

11. Click **Next**.
    myQNAPcloud applies your settings.
    The **Summary** screen appears.
12. Review the details, and then click **Finish**.

Installing myQNAPcloud Link

Only perform this task if you did not enable myQNAPcloud Link when registering your device to your myQNAPcloud account.

1. Log on to QNAP as administrator.
2. Open **App Center**.
3. Click .
   A search box appears.
4. Type `myQNAPcloud Link` and then press `ENTER`.
   The myQNAPcloud Link application appears in the search results list.
5. Click **Install**.
   App Center installs myQNAPcloud Link on your device.

Overview

The **Overview** screen displays your basic myQNAPcloud settings, as well as the device network connectivity and DDNS status.

Status Icon	Description
	The item is enabled and functioning properly.
	The item is disabled.
	One or more settings need to be configured for the item to function properly.
	There is no network connectivity.

Button	Description
	Click this to view your QNAP ID details.
	Click this to sign out of myQNAPcloud.
	Click this to modify your device name.
	Click this to copy the SmartURL to your clipboard.
	Click this to open the myQNAPcloud FAQ page on your browser.
	Click this to diagnose connection problems.

Button	Description
Test	Click this to test the internet connectivity.

Configuring UPnP Port Forwarding

UPnP allows your devices to automatically configure port forwarding settings and discover other devices on the network. Port forwarding is only available if your router supports UPnP.

Warning
Despite its convenience, UPnP may expose your device to public networks. This may allow malicious attackers to access your sensitive data, scan your private networks, and use your devices for DDoS attacks. To ensure your device and data security, we recommend disabling UPnP and manually configuring port forwarding settings on your router.

1. Go to **Auto Router Configuration**.
2. Enable **UPnP Port Forwarding**.
   A confirmation message appears.
3. Read the instructions carefully and understand the risks of enabling UPnP.
4. Select **Enable**.
   Your device scans for UPnP routers on the network.

Tip

- You can go to **Overview** to verify that there are no connectivity errors.
- If your device cannot locate the router, click **Rescan**. If the issue persists, click **Diagnostics**, and then verify your network configuration or contact QNAP support through **Helpdesk**.

5. Optional: Add a new service to the **Forwarded Services** table.
   a. Click **Add NAS Service**.
      The **Add NAS Service** window appears.
   b. Specify a NAS service name that contains 1 to 64 ASCII characters.
   c. Specify a port number.
   d. Select an external port setting.
      - **Automatic**: myQNAPcloud automatically selects an available external port.
      - **Manual**: You can specify a new port if the current service port is being used by other services.
   e. Select a protocol.
      If you are unsure about this setting, select **TCP**.
   f. Click **OK**.
6. In the **Forwarded Services** table, select the services you want to forward.
7. Click **Apply to Router**.

Configuring DDNS Settings

1. Open myQNAPcloud.
2. Go to **My DDNS**.
3. Enable **My DDNS**.
4. Perform any of the following tasks.

Task	User Action
Change the myQNAPcloud DDNS domain name	**a.** Click **here**. 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 **Manually configure your DDNS IP address**. The **Public IP Address** window appears. **b.** Select an option. • **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**.

Restarting DDNS Service

DDNS service may sometimes be disabled or suspended due to security concerns. You can restart the DDNS service in myQNAPcloud to regain access to the service.

1. Clear the cache on your web browser.
2. Log on to QuTS hero as administrator.
3. Open myQNAPcloud.
4. Go to **My DDNS**.
5. Disable **My DDNS**.
6. Enable **My DDNS**.

myQNAPcloud DDNS service is restarted and resumed.

Tip
If you still cannot connect to the NAS via myQNAPcloud DDNS, the service may be temporarily blocked by your Internet Service Provider (ISP). Wait at least two hours before attempting to restart the DDNS service.

Configuring Published Services

1. Open myQNAPcloud.
2. Go to **Published Services**.
3. In the **Publish** column, select all the services you want published.
   Published services are accessible through the myQNAPcloud website.
4. Optional: In the **Private** column, select all the services you want publish privately.
   Private services are only available to specified users with the access code.
   a. Specify an access code containing 6 to 16 alphanumeric characters.
   b. In the **User Management** table, select the users you want to grant access to.
      You can select a maximum of 9 users.

Tip
Click **Add Users** to add users to the list.
Click **Delete** to remove users from the list.

   c. Optional: Modify user access privileges.

Option	Description
myQNAPcloud Connect (VPN)	Select this option to grant users access to private NAS services when they use the myQNAPcloud Connect utility. Users can download myQNAPcloud Connect from the QNAP Utilities page (https://www.qnap.com/en/utilities/essentials).
myQNAPcloud Website	Select this option to grant users access to private NAS services published in the myQNAPcloud website (https://www.myqnapcloud.com/).

5. Click **Apply**.

Enabling myQNAPcloud Link

1. Open myQNAPcloud.
2. Go to **myQNAPcloud Link**.
3. Enable **myQNAPcloud Link**.

Tip
If there are issues with the connection, click **Reconnect**.

Configuring Device Access Controls

1. Open myQNAPcloud.
2. Go to **Access Control**.
3. Select an access control option.

Option	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 will not appear in the search results. Only you can access your device on the myQNAPcloud website.	Select **Private**.
Customized	Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL	**a.** Select **Customized**. **b.** Optional: Add a user. **1.** Click **Add**. **2.** Specify the user's email address or phone number. **3.** Click . **c.** Optional: Remove a user. • From the list of users, identify a user you want to remove. • Click ×.

4. Click **Apply**.

Installing an SSL Certificate

Important
myQNAPcloud SSL web service and Let's Encrypt certificates can only be used with the myqnapcloud domain.

1. Open myQNAPcloud.
2. Go to **SSL Certificate**.
3. Download and install a certificate.

Type	Description	User Action
myQNAPcloud SSL web service certificate	This certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users. You can purchase certificates on the myQNAPcloud website.	**a.** Under **myQNAPcloud SSL Certificate**, click **Download and install**. The **Download & Install SSL Certificate** window appears. **b.** Select a license from the list. A notification appears if you have not yet purchased a myQNAPcloud 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.	**a.** Under **Let's Encrypt**, click **Download and install**. The **Download & Install SSL Certificate** window appears. **b.** Specify a valid email address. This address is required for the Let's Encrypt account registration. **c.** Optional: Select **Automatically renew domain before expiration.**

4. Click **Confirm**.
   myQNAPcloud applies the certificate and displays the details.

Tip
To delete the certificate from the device, click **Release** and then **Confirm**.

12. App Center

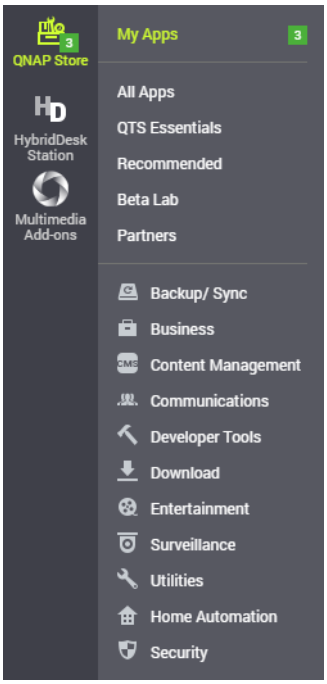
App Center is a digital distribution and management platform in QuTS hero where you can browse, download, and manage applications and utilities developed for the QNAP NAS.

Navigation

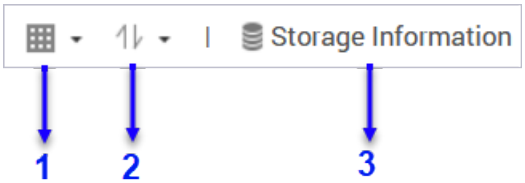
You can view all App Center apps in the left panel or configure a number of settings using the toolbar.

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 and select a view mode.

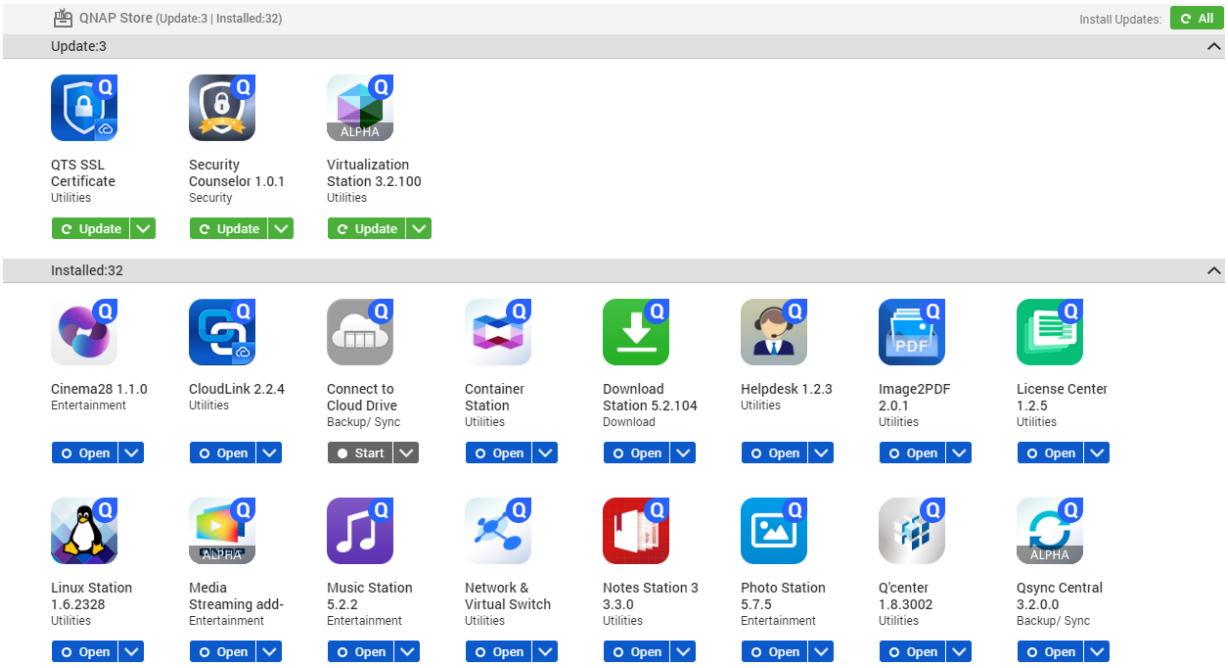
No.	Elements	Possible User Actions
2	App sorting	Click ˇ and select an app sorting method.
3	Storage information	View the basic storage pool information and the installation locations of your apps. For more storage pool information, click **Details**.

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 digital signature details
   - View the app changelog
   - Go to the QNAP forum
   - View the app tutorial
   - Download the app installation package

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 the app installed is invalid, it will immediately terminate app installation and request you to remove the app.

Important
Certain apps require activating a subscription or license before app installation. You can go to 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.
   The **Install Manually** window appears.
3. Click **Browse**.
4. Locate and select the installation package.
5. Click **Install**.

A message appears.

6. 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

You can migrate an installed app to another volume to better allocate system resources.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Migrate to**.
   The **App Migration** window appears.
5. Select the destination volume.
6. Click **Migrate**.
   A confirmation message appears.
7. Click **OK**.

Granting or Denying User Access to an App

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 mouse pointer 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
    - Every user's main menu and as an app shortcut on the login screen

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**.

App Center Settings

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
To protect the NAS from security vulnerabilities, QuTS hero by default will check for app updates every day.

1. Open App Center.
2. Click ⚙.
3. Go to **Update**.
4. Select **When updates are available** and then select one of the following options.

Option	Description
Send a notification	QuTS hero sends notification messages when updates are available for your apps. You can click **Configure 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. You can select how often App Center should check for available updates.
Install all required updates automatically	App Center automatically installs all required updates for your apps to ensure their functionality, compatibility, and data security. You can select how often App Center should check for required updates.

5. Select an automatic update detection frequency.
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 does not allow the installation of invalid apps, including apps with invalid digital signatures, apps unapproved by App Center, or from Software Store. If App Center detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.

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**.

13. 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 the item you want to buy, 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.
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. If you are using NAS devices running QuTS hero version 4.3.4 or older, use PAKs to activate licenses through License Center. If you are using NAS devices running QuTS hero version 4.3.4 or later, you can transfer PAKs purchased from the Old QNAP License Store to NAS devices. For details, see Activating a License Using a Product Key or PAK.
Offline	Use this method when the NAS is not connected to the internet. For details, see Activating a License Offline.

Activating a License Using QNAP ID

Before activating your license, ensure the following.

- Your 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.
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.

Method	Steps
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 NAS 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 NAS 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 NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using an Unused License.
Offline using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you have a valid, unused product key for a subscription-based license, and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using a Product Key.

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**.

Payment Method	User Action
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.
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 NAS is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **My Licenses**.

3. Identify the license you want to transfer, and then click .
   A confirmation message appears.
4. Read the terms of service, and then click **Transfer & Activate**.

Warning
After you register a license with your current QNAP ID, it will no longer be transferable.

License Center transfers the license.
A confirmation message appears.

5. Optional: Click **QNAP License 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.

14. Multimedia

QuTS hero provides a range of applications and utilities for viewing, playing, and streaming multimedia files stored on the NAS.

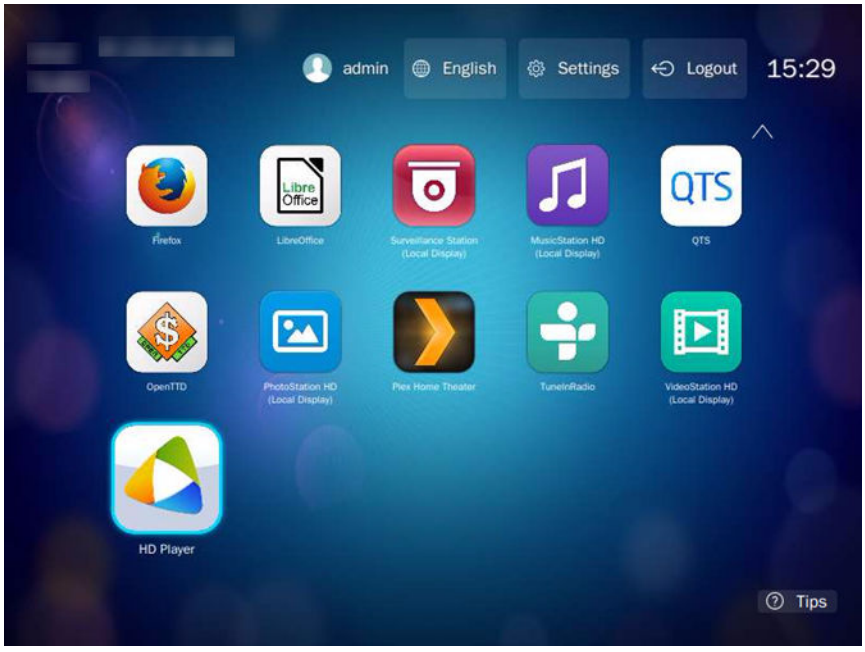
Application/Utility	Description
HybridDesk Station (HD Station)	Connect to an HDMI display to access multimedia content on your NAS.
DLNA Media Server	Configure your NAS as a Digital Living Network Alliance (DLNA) server to access media files on your NAS from devices on your home network.
Media Streaming 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**.

Action	Steps
Remove HD Station and related applications	**a.** Click **Remove**. A dialog box appears. **b.** Click **OK**.
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 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.

The contents displayed in DLNA Media Server are based on user account permissions and Multimedia Console settings.

Important
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.

1. Go to **Control Panel** > **Applications** > **DLNA Media Server** .
2. Select **Enable DLNA Media Server**.
3. Optional: Specify the following information.

Field	Description
Service Name	Specify a name for the DLNA Media Server.
Select default user account	Select the user account that will be the directory for the DLNA Media Server.

4. Click **Apply**.

Configuring DLNA Media Server

1. Go to **Control Panel** > **Applications** > **DLNA Media Server** .
2. Perform any of the following actions.

Action	Steps
Scan for multimedia content	Click **Scan now**.
Restart DLNA Media Server	Click **Restart**.

Action	Steps
Configure advanced settings	**a.** Click **Advanced Settings**. The **Media Streaming Add-on** portal opens in a new browser window. **b.** Configure the settings. **Note** Media Streaming Add-on must be installed to configure advanced settings. For details, see Media Streaming Add-on.

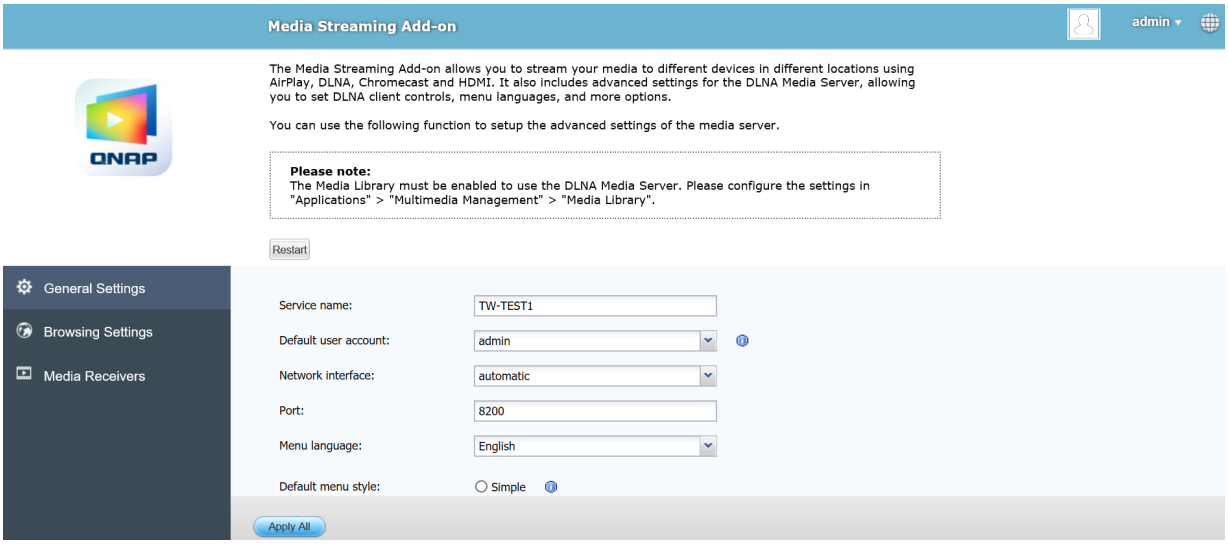
Media Streaming Add-on

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.
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.

Setting	Description
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

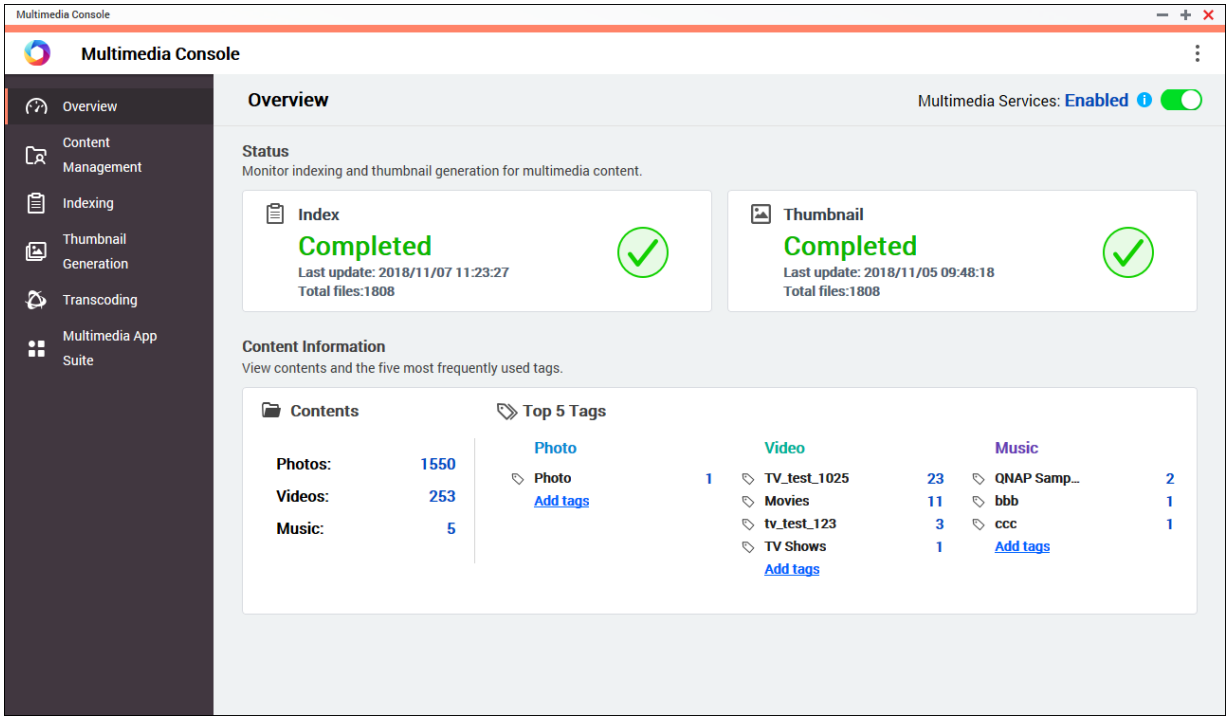
Multimedia Console helps you manage installed multimedia apps and content stored on the NAS. Multimedia Console can index files, transcode videos, and generate thumbnails for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Server.

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

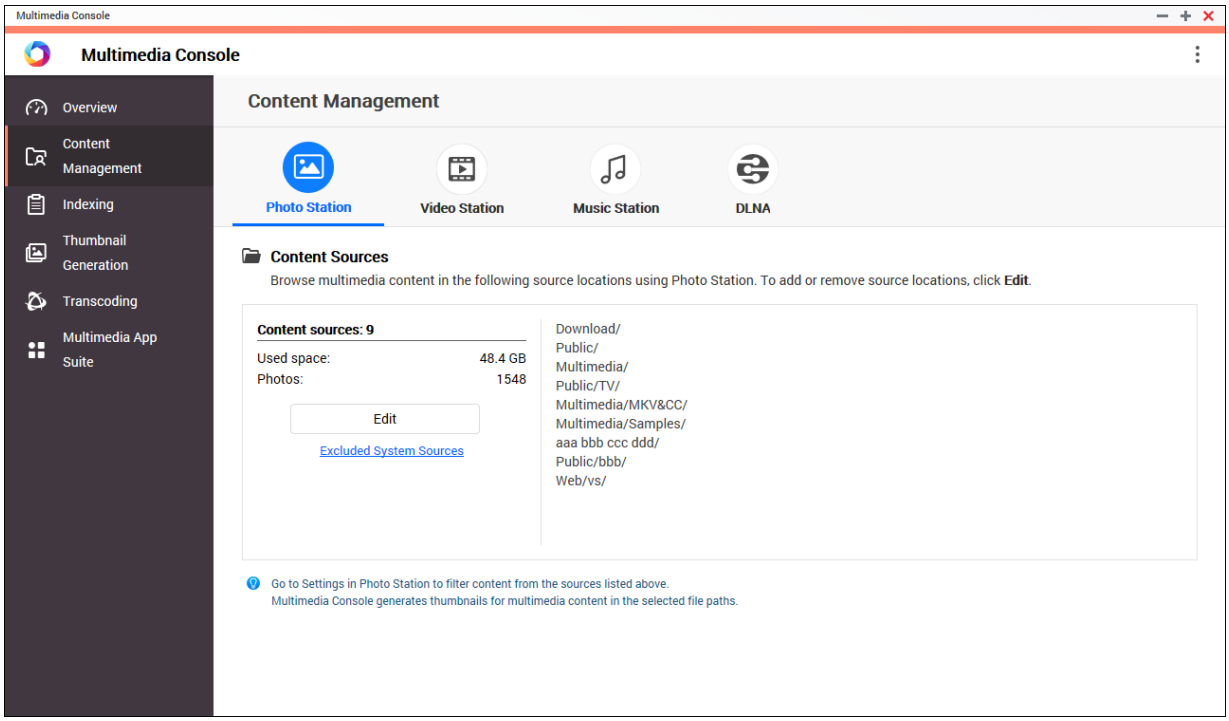
Important
To use third-party applications and Multimedia Console features like indexing and thumbnail generation, Multimedia Services must be enabled.

Tip
You can enable or disable Multimedia Services in the upper right of the **Overview** screen.



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.



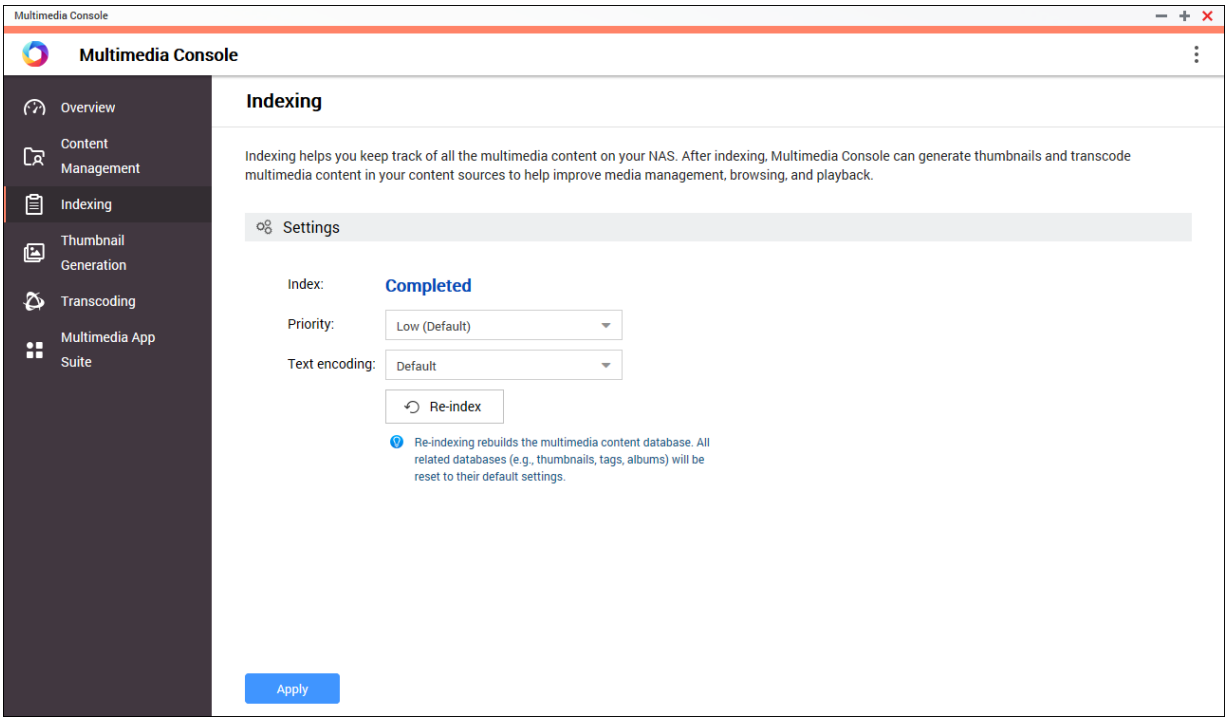
Editing Content Sources

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.



Configuring Indexing Settings

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**.

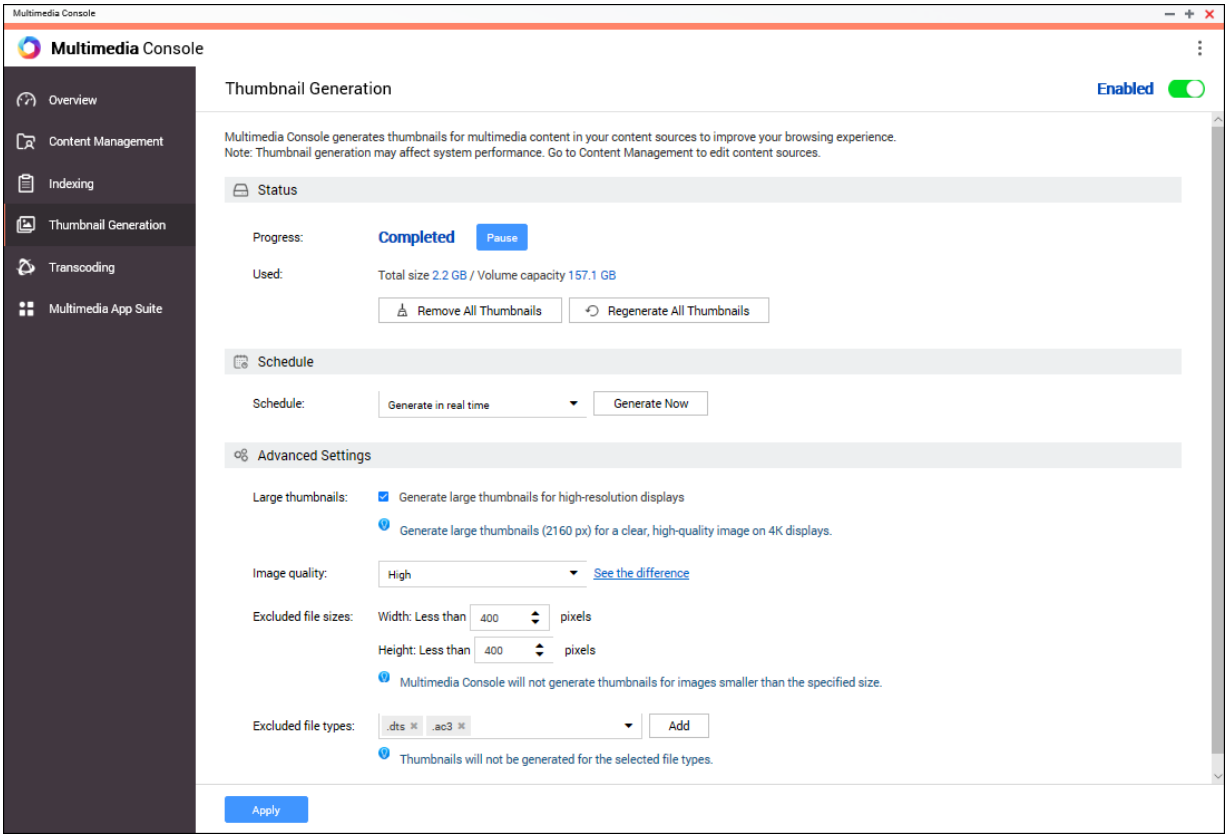
Tip
Click **Re-index** to rebuild the multimedia content database and revert dependent databases to their default settings.

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.



Configuring Status

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 **Progress**, 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 **Progress**, 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 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 for new files as soon as they are detected.

Option	Description
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 only after clicking **Generate Now**.

Tip
Click **Generate Now** to force Multimedia Console to start generating thumbnails immediately.

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
Large thumbnails	When selected, Multimedia Console generates high-resolution thumbnails (2160 px) for media files.
Image quality	Select **High** or **Low**. **Tip** Click **See the difference** to view a side-by-side comparison of high- and low-quality thumbnails.
Excluded file sizes	Multimedia Console only generates thumbnails for images that are larger than the specified resolution.
Excluded file types	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.

Overview

You can manage Background Transcoding and On-the-Fly Transcoding tasks from the Overview tab on the **Transcoding** screen.

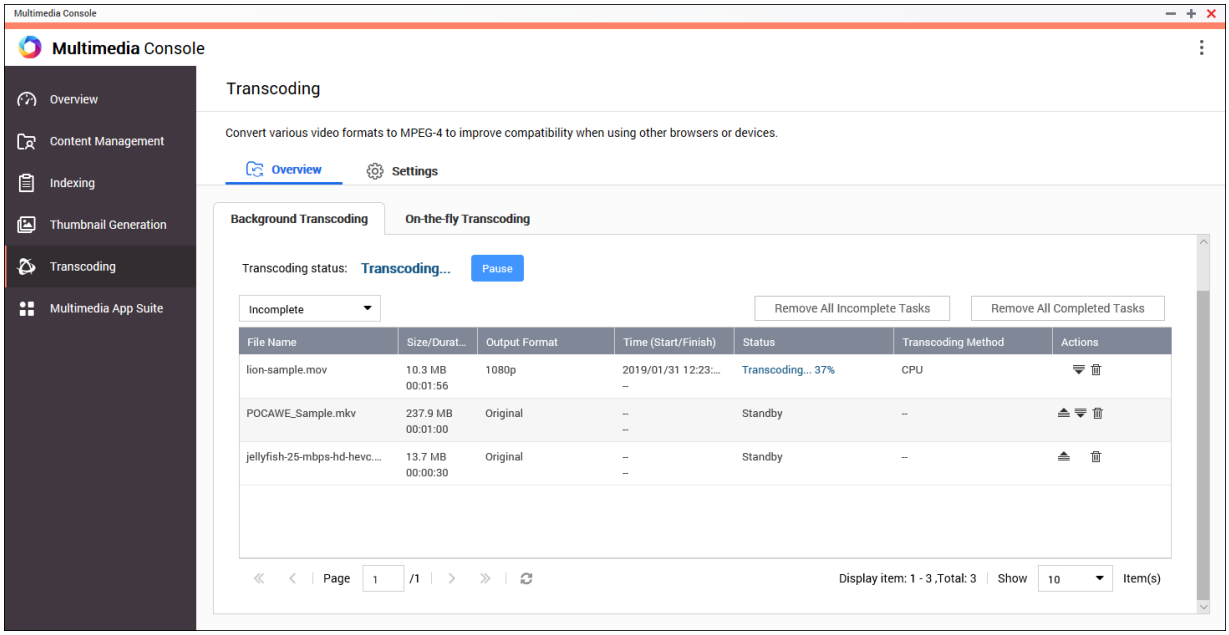
Note

- Transcoding is only available for certain NAS models. Go to https://www.qnap.com/en/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. 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. **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.
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.

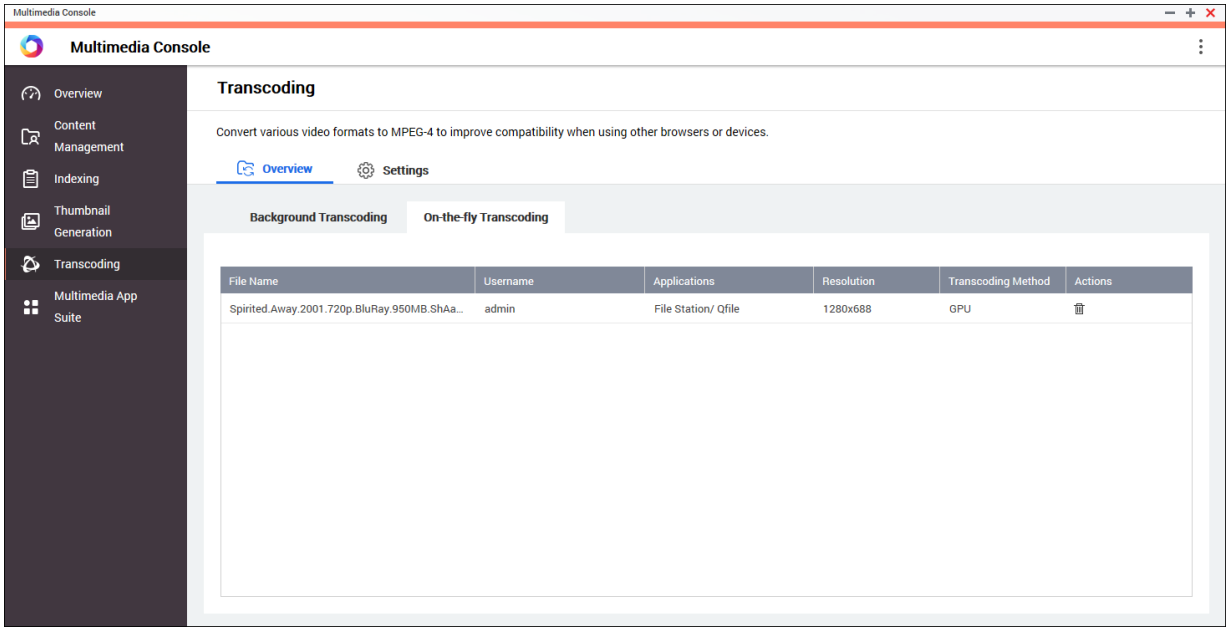
Task	User Action
Remove incomplete tasks	1. Click **Remove All Incomplete Tasks**. A dialog box appears. 2. Click **OK**.
Remove completed tasks	1. Click **Remove All Completed Tasks**. A dialog box appears. 2. Click **OK**.

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

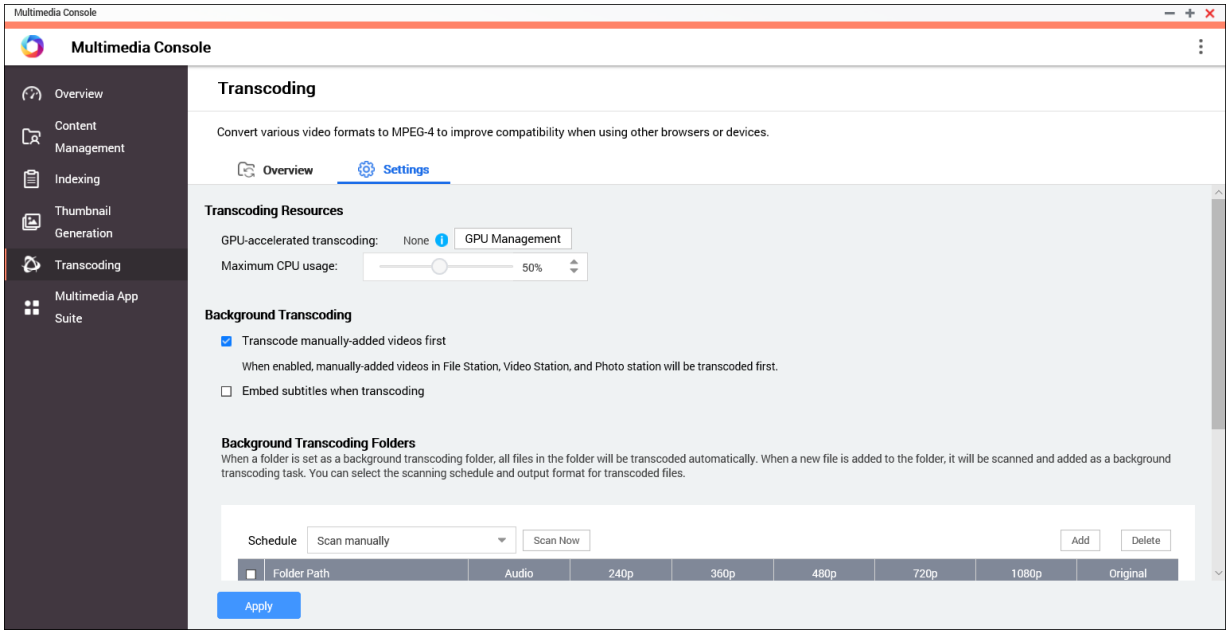
The On-the-Fly Transcoding tab displays information about on-the-fly transcoding tasks. You can view and manage on-the-fly transcoding tasks from this tab.



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**.

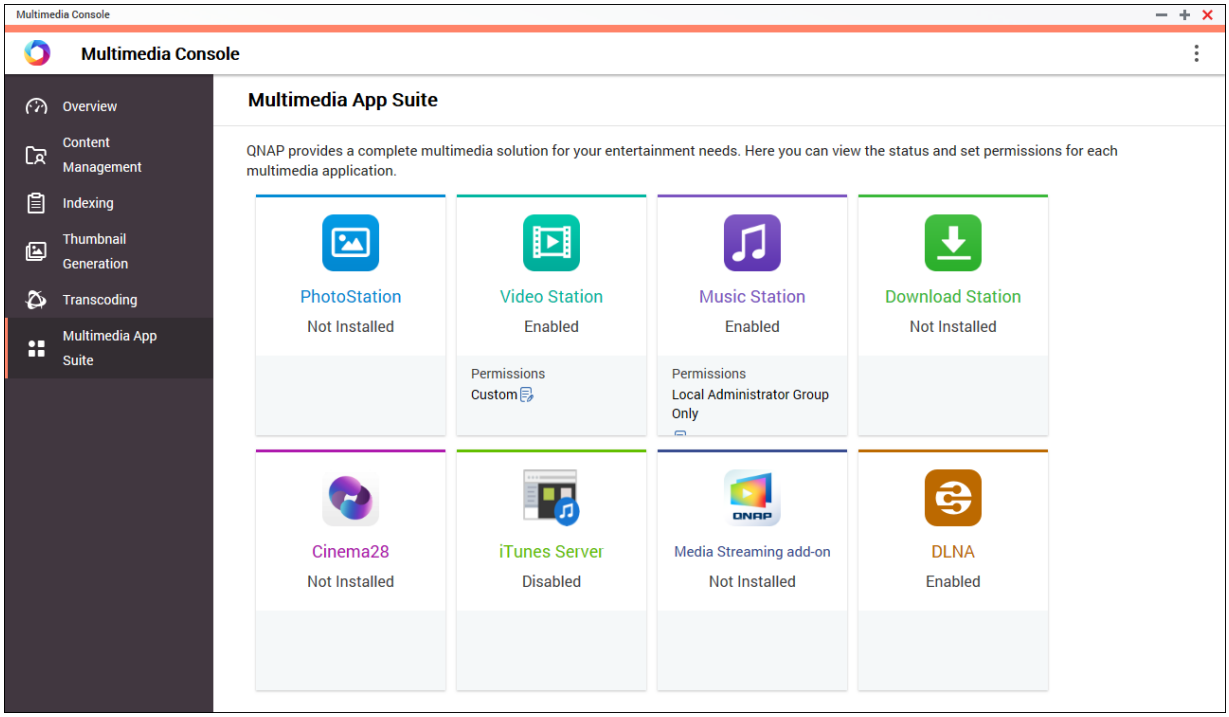
Configuring Background Transcoding Folders

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 + Install.
Enable an app or service	**a.** Locate an app or service with the status **Disabled** under the app or service name. **b.** Click **Disabled**. **c.** The app or service opens in a new window. **d.** Enable the app or service.
Disable an app or service	**a.** Locate an app or service with the status **Enabled** under the app or service name. **b.** Click **Enabled**. **c.** The app or service opens in a new window. **d.** Disable the app or service.

Configuring Multimedia App Permissions

1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.
3. Locate an app with access permissions.
4. Under **Permissions**, click the permission status.
   The **Permission Settings** window opens.
5. Select a permission type.

Permission Type	Description
All Users	All users can access the app.
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**.

15. 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** .

Monitoring System Logs

The **Overview** screen provides statistical graphics to help you visualize system log data and monitor device status.

System Event Log

The **System Event Log** tab provides the following widgets to visualize the statistical data of the system event logs from your devices.

Important
You must configure a log destination to enable the system event log feature.
For details, see Configuring Event Log Settings.

Tip
The System 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 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 Applications for Error Logs	This widget displays the five applications that have the largest numbers of error log entries.
Top 5 Applications for Warning Logs	This widget displays the five applications that have the largest numbers of warning log entries.

System Access Logs

The **System Access Log** tab provides the following widgets to visualize the statistical data of the system access logs from your devices.

Tip
The System 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 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 logins 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 Logs

Local Device Logs allows you to monitor system event logs, system access logs, and online user status on one local device. You can also configure log filters, log settings, and remove event indicators.

Local System Event Logs

You can monitor and manage system event logs from local devices in **Local Device** > **System Event Log** .

Important

- You must configure a log destination to enable the local system 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.

On the **System 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 Display Settings.
Export logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Export**. **3.** Select an export file format. **Note** 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. **Note** 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 System Event Log.
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, see Creating an Event Notification Rule.
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. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 2. Click **Select all**.

Task	Steps
Invert selection	1. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 2. 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 System Access Logs

You can monitor and manage system access logs from local devices in **Local Device** > **System Access Log** .

Important

- You must configure a log destination to enable the system 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.

On the **System 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.

Task	Steps
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 Display Settings.
Export logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Export**. **3.** Select an export file format. **Note** 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. **Note** 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. 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 System Access Log.
Select display items	1. Click +. 2. Select the item category to display.
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.

Viewing Online Users

On the **Online Users** screen, you can see the list of online users and their detailed information, such as login date, login time, username, source IP address, and connection type.

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.
Select the items to display on the list	**1.** Click . **2.** Select the item category to display.

Creating a Custom Filter Tab for Local Device System Logs

You can create custom filter tabs for Local System Event Logs and Local System 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 System Event Log
- Creating a Custom Filter Tab for Local System Access Log

Creating a Custom Filter Tab for System Event Log

1. Open QuLog Center.
2. Go to **Local Device** > **System 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.

Fields	Steps
Application	**a.** Click ▾. The application drop-down menu appears. **b.** Select an application. The **Category** option appears. **Note** The **Category** option only appears when you specify the application. **c.** Specify the application **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.

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 System Access Log

1. Open QuLog Center.

2. Go to **Local Device** > **System 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.

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 system event logs.

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Event Log Settings** .
3. Specify the following settings:

Settings	Steps
Destination	**a.** Click ▾ . The log destination option drop-down menu appears. **b.** Select a log 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.
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.

Settings	Steps
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 system 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	**a.** Click ▾. The log destination option drop-down menu appears. **b.** Select a log 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.

Settings	Steps
Maximum number of entries	**a.** Click ▾. The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed.
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 event logs.
   a. Click **Delete All Access Logs**.
   A confirmation message appears.
   b. Click **Yes**.

Warning
You cannot restore deleted logs.

5. Click **Apply**.

Configuring Display Settings

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:

Accessing Display Setting Method	Steps
System Event Log	Go to **Local Device** > **System Event Log** > **Display style** .
System Access Log	Go to **Local Device** > **System 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**.

Task	Steps
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**.
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 condition	**a.** Select a display style. **b.** Select a condition from the list. **c.** Click **Delete**. A confirmation message appears. **d.** Click **Yes**.

Task	Steps
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 system event logs and system 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**. System 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**. System 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:
   - **Destination IP**

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 multiple 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 system 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 **System Event Log** or **System 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 **System Event Log** or **System Access Log**.
4. Click **Add Filter Criteria**.
   The filter criteria window appears.
5. Specify the following information:

Log Type	Settings
System Event Log	• Severity level • User • Source IP • Application • Category • Content • Hostname
System Access Log	• Severity level • User • Source IP • Accessed resources • Hostname • Connection type • Action

6. 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 **System Event Log** or **System 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** > **QuLog Server** > **Filter Criteria** .
3. Select **System Event Log** or **System 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 **System Event Log** or **System 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 System Event Log on a Sender Device
- Creating a Custom Filter Tab for System Access Log 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 System Event Logs on the Log Receiver

You can monitor and manage system event logs received by the **Log Reciever** in **QuLog Service** > **All Devices** > **System Event Log** . You can also monitor system 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 **System 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. • **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 Display Settings.
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. **Note** 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. **Note** 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.** 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 System Event Log on the Sender Device.
Select display items	**1.** Click . **2.** Select the items to display.

Task	Steps
Select all log entries	1. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 2. Click **Select all**.
Invert selection	1. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 2. 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 System Access Logs on the Log Receiver

You can monitor and manage system access logs received by the **Log Receiver** in **QuLog Service** > **All Devices** > **System Access Log** . You can also monitor system 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 **System 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.

Task	Steps
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 Display Settings.
Export logs	**1.** Click . The **Export Logs** window appears. **2.** Select an export file format. **3.** Specify the maximum number of log entries per file. **4.** Optional: Compress the export file and specify a password. **5.** Click **Export**.
Download exported logs	**1.** Click . The **Export Logs** drop-down menu appears. **2.** Click **Download**. **3.** Select an export file format. **Note** 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.** 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 System Access Log on the Sender Device.
Select display items	**1.** Click . **2.** Select the items to display.
Select all log entries	**1.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **2.** Click **Select all**.

Task	Steps
Invert selection	1. Click **Select multiple entries**. The select multiple entries drop-down menu appears. 2. 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 Configuriing Log Sender Settings.

Creating a Custom Filter Tab for System Event Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices** .
3. Click on a sender device.
4. Go to **System 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.
Application	**a.** Click ▾. The application drop-down menu appears. **b.** Select an application. The **Category** option appears. **Note** The **Category** option does not appear if you select any applications or do not specify the application. **c.** Specify the application **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.

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 System Access Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices** .
3. Click on a sender device.
4. Go to **System 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.

Fields	Steps
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.

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. Click **Event Indicators**.
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 system access logs, QuLog Service system event logs, and QuLog Service system access logs.

Configuring Notification Rule Settings

QuLog Center can send notifications to recipients when the **Log Receiver** receives system event logs or system 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	**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. **Important** You must select the **Log filter criteria** option in **System Notification Rules** when creating QuLog Center notification rules for receiving local device logs, QuLog Service system event logs, and QuLog Service system access logs. To enable the **Log filter criteria** option, go to **Notification Center** > **System Notification Rules** > **QuLog Center** > **Log Filter Criteria** . **b.** Click **Apply**. The notification rule is created.
Edit a notification rule	Click .
Enable or disable a notification rule	Click toggle.
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 system access logs, QuLog Service system event logs, and QuLog Service system 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. Specify the following information:

Log Type	Settings
System Event Log	• Severity level • User • Source IP • Application • Category • Content • Hostname
System Access Log	• Severity level • User • Source IP • Accessed resources • Hostname **Note** This option is only available for QuLog Service devices. • Connection type • Action

6. 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** .

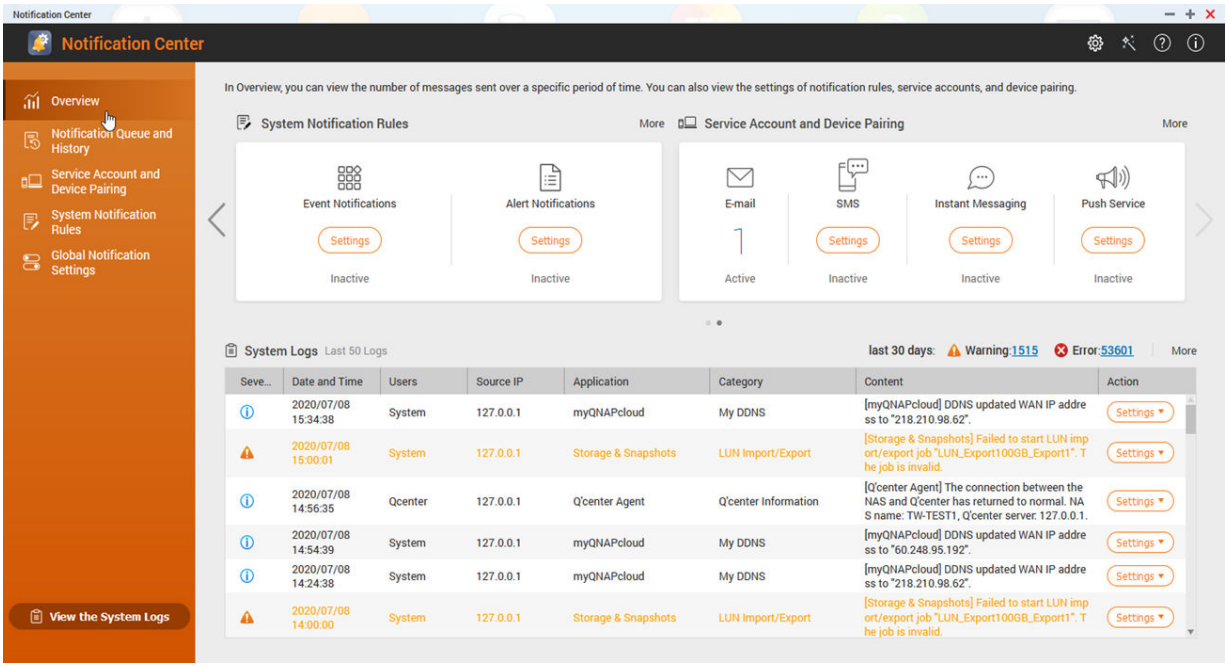
3. Select a filter criteria.
4. Click .
   A confirmation message window appears.
5. Click **Yes**.
   The filter criteria is removed.

16. 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. You can send notifications to recipients through different channels including emails, SMS, instant messaging, and other push services. Notification Center also lets you create custom notification rules and criteria, ensuring that you receive notifications that are most relevant to your needs.

Overview

The **Overview** screen displays the number of notifications delivered over a specific period of time. It also displays the number of notification rules, service accounts, and paired devices you configured.



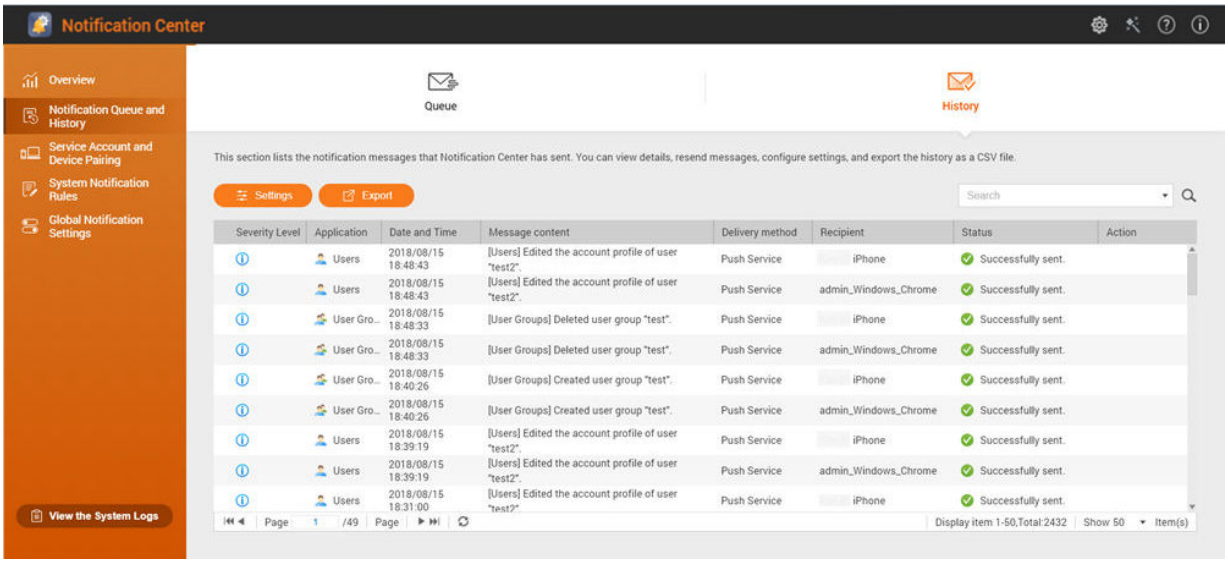
Notification Queue and History

Queue

The **Queue** screen displays the messages that Notification Center is going to send. The required transmission time depends on the current status of your NAS. You can remove a message from the queue before it is sent. Messages removed from the queue will not appear in the **History** screen.

History

The **History** screen displays the messages that Notification Center has sent. You can view details, resend messages, configure settings, and export the history as a CSV file. In the settings, you can specify how long your notification records are retained and where they are stored.



No.	Task	User Action
1	Export the notification message history.	Click **Export**. Notification Center saves the CSV file on your computer.
2	Resend the notification.	Identify the notification you want to resend, and then click . This button only appears when Notification Center is unable to send the notification to the recipient.

Configuring History Settings

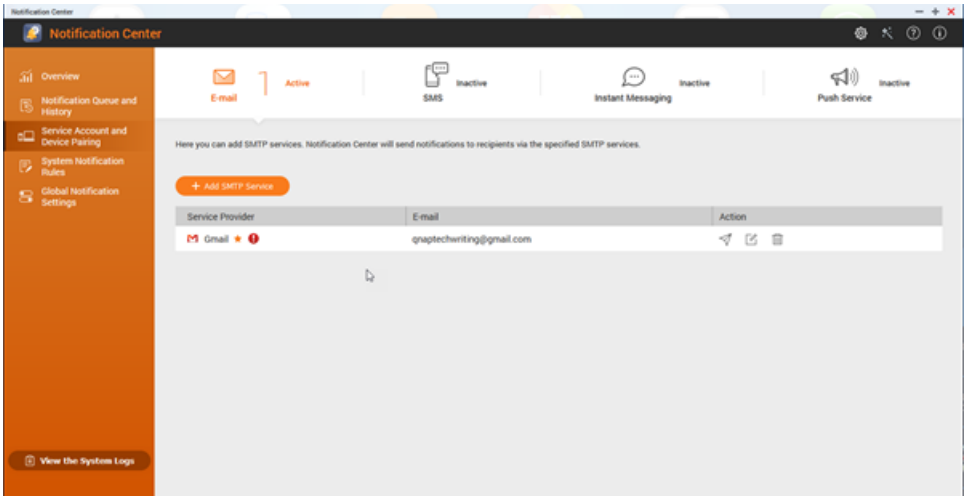
1. Open Notification Center.
2. Go to **Notification Queue and History** > **History** .
3. Click **Settings**.
   The **Settings** window appears.
4. Configure the following information.
   - Retention period: Specify the maximum number of days Notification Center retains notification records before deleting them.
   - Notification record storage: Select whether or not you want to keep notification records in a specified local folder.
5. Click **Confirm**.
   Notification Center saves your settings.

Service Account and Device Pairing

Service Account and Device Pairing allows you to configure the simple mail transfer protocol (SMTP) and short message service center (SMSC) settings so you can receive notifications through email and SMS. You can also pair your instant messaging accounts and devices with your NAS to receive notifications through instant messaging or push services.

Email Notifications

The Email screen allows you to add and view email notification recipients and configure your simple mail transfer protocol (SMTP) service settings.



Button	Task	User Action
	Send a test message to a specified recipient.	1. Click . 2. Specify an email address. 3. Click **Send**.
	Edit the configurations of an existing email server.	1. Click . The **Edit SMTP Service Account window** appears. 2. Edit the settings. 3. Click **Confirm**.
	Remove 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**.
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**.
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 you authenticate an email server account using **Browser Station**, please ensure the following:

- You have **File Station** access permission.
- Your device is compatible with **Browser Station**.
  For details, see How to Use Browser Station.
- **Browser Station** is installed on your device.
  For details about installation requirements, see How to Use Browser Station.
- **Container Station** is installed on your device.
- If you are using a proxy server to access **Browser Station**, the proxy server must support WebSocket.

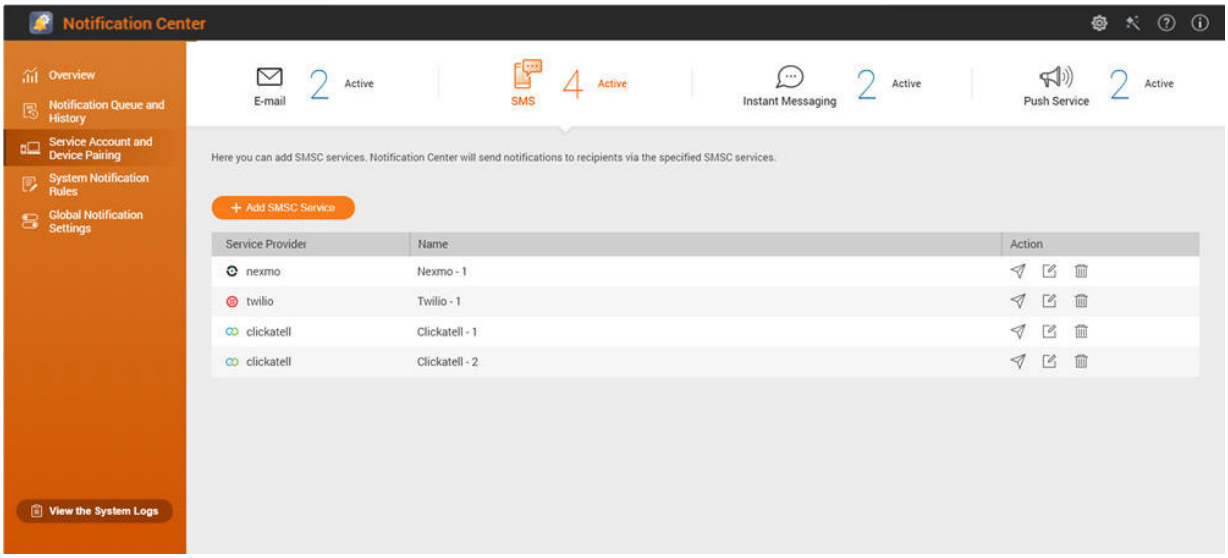
1. Go to **Service Account and Device Pairing** > **E-mail** .
2. Click **Add SMTP Service**.
   The **Add SMTP Service** window appears.
3. Click **Authenticate with Browser Station**.
   The **Browser Station** window appears.

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 your short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Nexmo, and Twilio.



Button	Task	User Action
	Send a test message to a specified recipient.	1. Click . The **Send test message** window appears. 2. Specify a country code and phone number. 3. Click **Send**.
	Edit the configurations of an existing SMS server.	1. Click . The **Edit SMSC Service Account window** appears. 2. Edit the settings. 3. Click **Confirm**.
	Remove an email server.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Configuring an SMS Notification

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
Nexmo	Nexmo API key and secret question, and a sender name The sender name can contain a maximum of 32 characters.
Twilio	Your Twilio account SID, access token, and the Twilio-provided phone number linked to your account

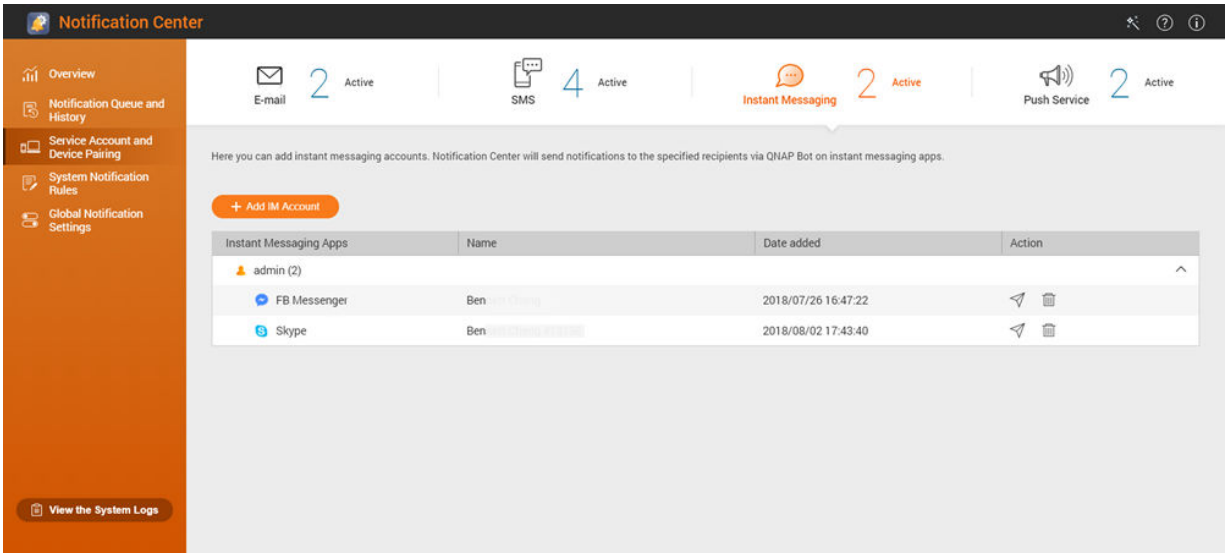
Custom	• URL template text formatted according to the format specified by your SMS service provider.
	Use the following replaceable URL template parameters.
	  • `@@UserName@@`: Specify the username for this connection.
	  • `@@Password@@`: Specify the password for this connection.
	  • `@@PhoneNumber@@`: Specify the phone number where the SMS messages are sent. This parameter is required.
	  • `@@Text@@`: Specify the text content of the SMS message. This parameter is required.
	Important
	You will not be able to receive SMS messages if the template text does not match the format used by your SMS service provider.
	• The name of the service provider. The name can contain a maximum of 32 ASCII characters.
	• A password. The password can contain a maximum of 32 ASCII characters.

Tip
To configure multiple SMS servers, click **Add SMSC Service**, and then perform the previous steps.

6. Click .
   The SMS server sends a test message.
7. Click **Create**.
   Notification Center adds the SMTP service to the list.

Instant Messaging Notifications

The Instant Messaging screen allows you to pair Notification Center with instant messaging accounts such as Skype and Facebook Messenger. Notification Center sends notifications to the specified recipients through QBot, the QNAP instant messaging bot account.



Button	Task	User Action
	Send a test message.	Click .
	Unpair from and remove the instant messaging account.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Skype account.
- Skype is installed on your device.

1. Go to **Service Account and Device Pairing** > **Instant Messaging** .
2. Click **Add IM Account**.
   The **Notification IM Wizard** appears.
3. Select Skype.
   The **Add Bot to Contacts** window appears.
4. Log in to the Skype account you want to pair.
   Skype adds QNAP Bot as a contact.
5. Close the **Add Bot to Contacts** window.
6. Click **Next**.
   A verification code appears.
7. On Skype, enter the verification code.

Notification Center verifies and pairs with the Skype account.

8. Click **Finish**.
   Notification Center adds the Skype account to the list.

Pairing Notification Center with Facebook Messenger

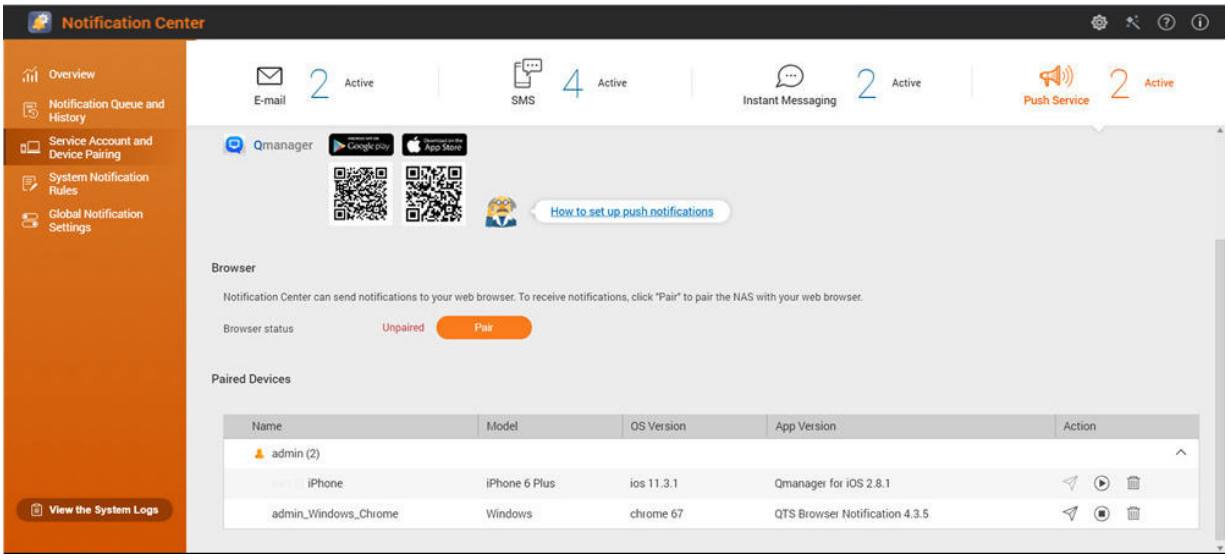
Before configuring instant messaging (IM) notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Facebook Messenger account.

1. Go to **Service Account and Device Pairing** > **Instant Messaging** .
2. Click **Add IM Account**.
   The **Notification IM Wizard** appears.
3. Select Facebook Messenger.
   The **Add Bot to Contacts** window appears.
4. Log in to the Facebook Messenger account you want to pair.
   Facebook Messenger adds QNAP Bot as a contact.
5. Click **Get Started**.
   A verification code appears on the **Notification IM Wizard**.
6. On Facebook Messenger, enter the verification code.
   Notification Center verifies and pairs with the Facebook Messenger account.
7. Click **Finish**.
   Notification Center adds the Facebook Messenger account to the list.

Push Notifications

The Push Service screen allows you to configure push services for web browsers and mobile devices.



Button	Task	User Action
	Send a test message.	Click .
	Start sending push notifications to the device or browser.	Click .
	Stop sending push notifications to the device or browser.	Click .
	Unpair and remove the device or browser.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Pairing Notification Center with a Mobile Device

Before starting pairing, ensure that the following requirements are met.

- 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 starting pairing, ensure that the following requirements are met.

- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers:

- Chrome 42 (or later versions)
- Firefox 50 (or later versions)

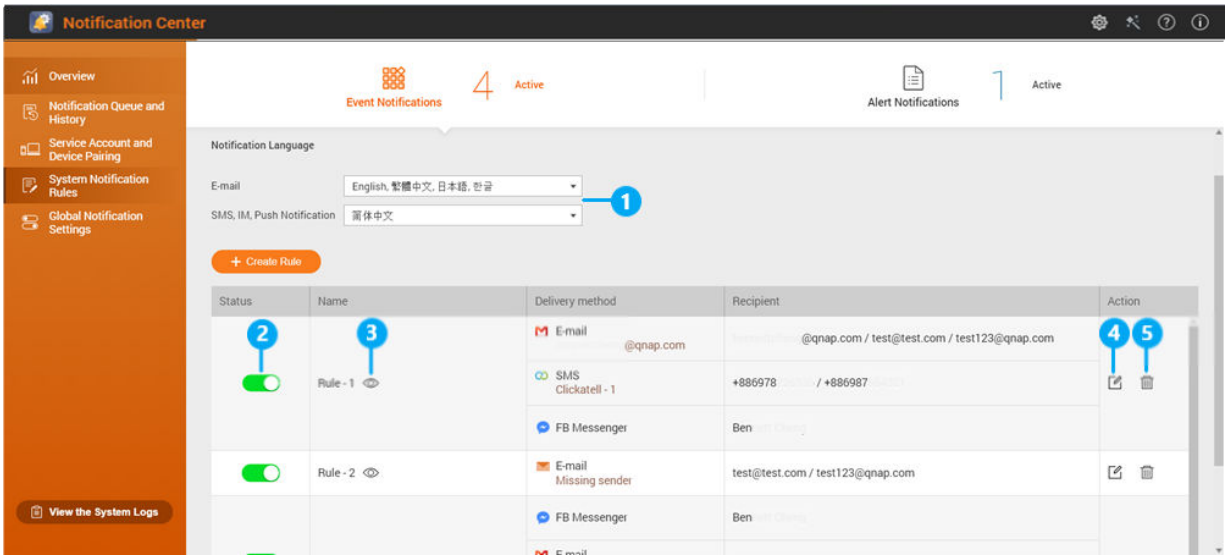
1. Go to **Service Account and Device Pairing** > **Push Service** .
2. Under Browser, click **Pair**.
   Notification Center pairs with your current browser.
   The browser appears in the list of paired devices.
3. Change your browser name.
   a. Beside your browser name, click .
   b. Specify a browser name.
      The field accepts a maximum of 127 ASCII characters.
   c. Press ENTER.
      Notification Center saves your browser name.

System Notification Rules

You can create and manage event notification rules to receive event notifications promptly.

Managing Event Notification Rules

You can create custom rules and select applications and features that you want to receive event notifications from. You can also specify the message type, keywords, and time range to further define notification types or narrow the scope. Notification Center supports sending event notifications in multiple languages and provides four delivery methods to meet your different needs, including emails, SMS, instant messaging, and push services.



No.	Tasks	User Actions
1	Specify a notification language.	1. Select one or more languages for email notifications. 2. Select a language for SMS, IM, and push notifications.

No.	Tasks	User Actions
2	Enable or disable the rule.	Click .
3	Preview the rule settings.	1. Click . The **Event Notifications** window appears. 2. Review the settings, and then click **Close**.
4	Edit the rule.	1. Click . The **Edit Rule for Event Notifications** window appears. 2. Edit the settings. 3. Click **Confirm**.
5	Delete the rule.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Creating an Event Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. Go to **System Notification Rules** > **Event Notifications** .
2. Click **Create Rule**.
   The **Create event notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.

Tip
To select all events, select **Select all**.
To display only the events for a specific application or service, select the item from the **Displayed Items** drop-down menu.

5. Click **Next**.
6. Select a 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.

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.
Instant Messaging or Push Service	Notification Center automatically assigns Qbot.

12. Configure the recipient information.

Method	User Action
Email	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **Tip** • To add a recipient, click **Add**, and then specify their email address. • To delete a recipient, click .
SMS	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then specify their cell phone number. • To delete a recipient, click .
Instant Messaging	Select one or more recipients. **Tip** To add instant messaging notification recipients, see the following topics: • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	Select one or more recipients. **Tip** To add push notification recipients, see the following topics: • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

13. Optional: Click to send a test message.
14. Optional: Click **Add Pair** to create a new pair.
15. Click **Next**.
16. Verify the rule settings.

17. Click **Finish**.
    Notification Center displays the new rule on the **Event Notifications** screen.

Creating an Alert Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. Go to **System Notification Rules** > **Alert Notifications** .
2. Click **Create Rule**.
   The **Create alert notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.
   a. Select a severity level.

Severity Level	Description
Information	Information messages inform users of changes in the NAS settings or its applications.
Warning	Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features.

   b. Optional: Specify a keyword filter.

Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click +, and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click +, and then specify one or more keywords.

Important
The alert notification filter only accepts keywords that are in English.

5. Optional: Specify a time range when you want to receive notifications.
6. Optional: Specify a notification message threshold.
7. Click **Next**.
8. Select a delivery method.
9. Configure the sender information.

Method	User Action
Email	**a.** Select an SMTP server. **Tip** To add an SMTP server, see Configuring an Email Notification Server. **b.** Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive. **c.** Optional: Select **Send email as plain text**.
SMS	Select an SMSC server. **Note** To add an SMSC server, see Configuring an SMS Notification Server.
Instant Messaging or Push Service	Notification Center automatically assigns Qbot.

10. Configure the recipient information.

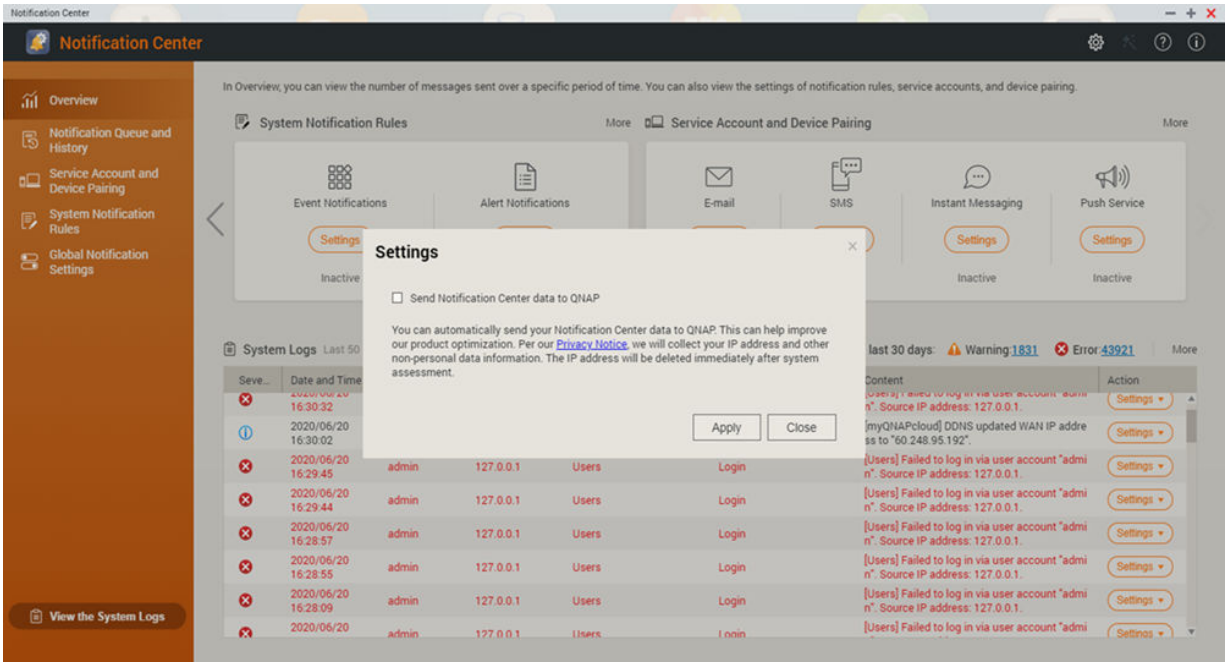
Method	User Action
Email	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **Tip** • To add a recipient, click **Add**, and then specify their email address. • To delete a recipient, click .
SMS	**a.** Click **Select NAS User**. The **Select NAS User** window appears. **b.** Select one or more NAS users. **c.** Click **Finish**. The **Select NAS User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then specify their cell phone number. • To delete a recipient, click .

Method	User Action
Instant Messaging	Select one or more recipients. **Tip** To add instant messaging notification recipients, see the following topics: • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	Select one or more recipients. **Tip** To add push notification recipients, see the following topics: • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

11. Optional: Click to send a test message.
12. Optional: Click **Add Pair** to create a new pair.
13. Click **Next**.
14. Verify the rule settings.
15. Click **Finish**.
    Notification Center displays the new rule on the **Alert Notifications** screen.

Settings

The **Settings** screen allows you to enable or disable submitting Notification Center data to QNAP. Click to open the **Settings** window.



Enabling Send Notification 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**.

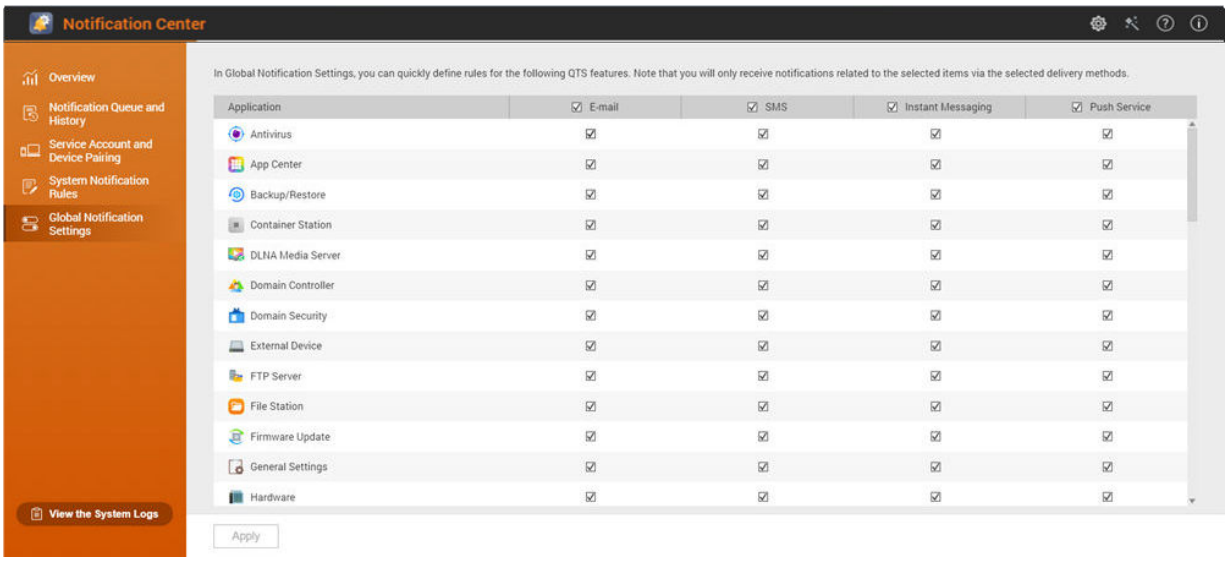
Disabling Send Notification Data to QNAP

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**.

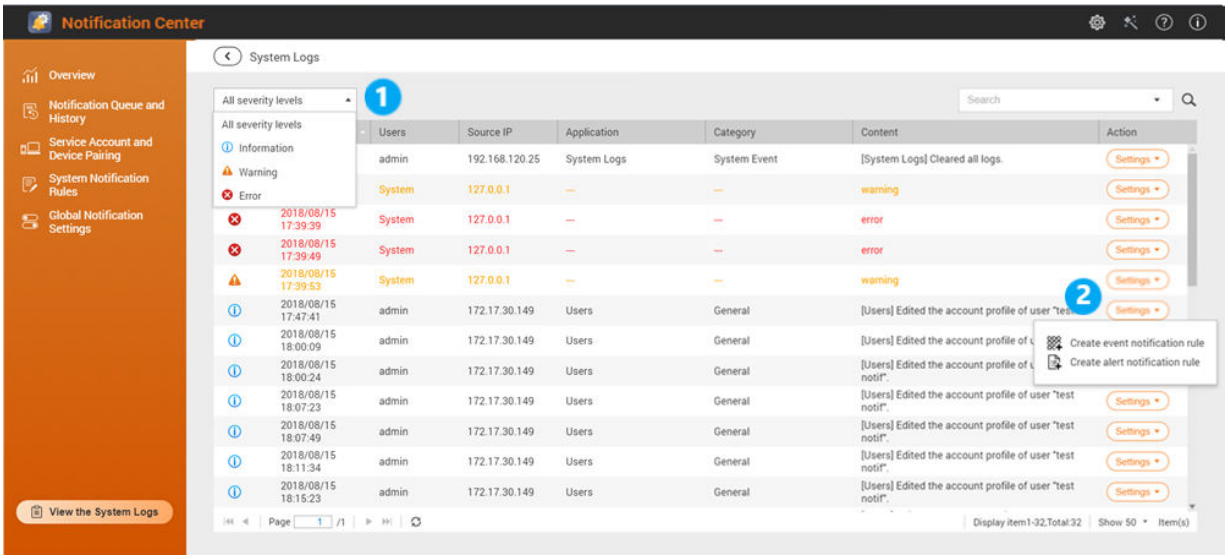
Global Notification Settings

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.



System Logs

The **System Logs** screen displays all system events on the NAS. On this screen, you can sort and filter the logs or create notification rules based on existing logs.



No.	Task	User Action
1	Filter system logs	Select a severity level.

No.	Task	User Action
2	Search system 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 **3.** Click **Search**. Lists all log entries that meet the specified conditions.
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**. **Tip** To add or edit notification rules, see the following topics: • Creating an Event Notification Rule • Creating an Alert Notification Rule

17. Malware Remover

About Malware Remover

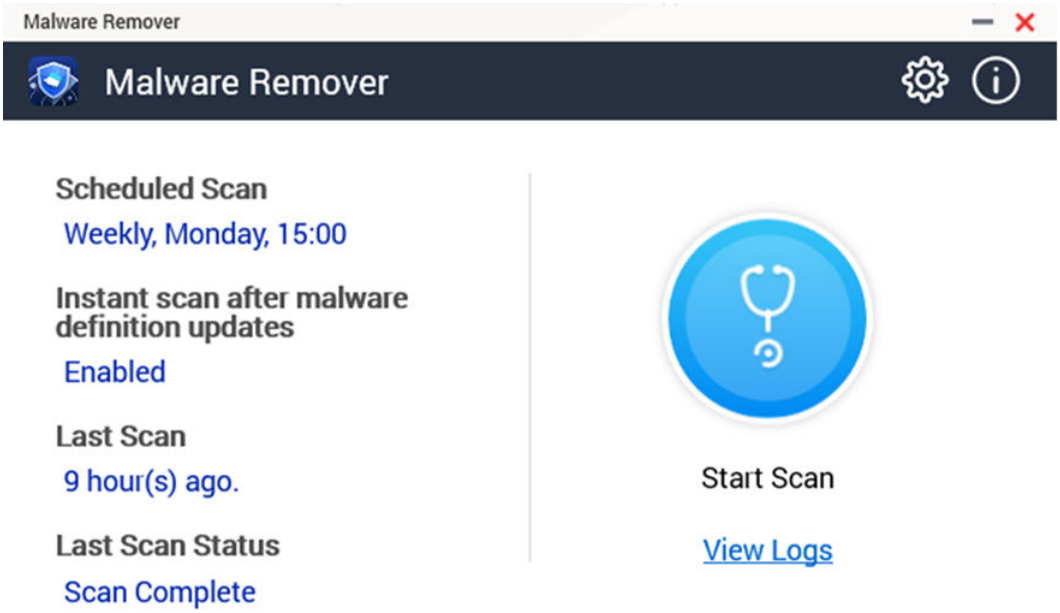
Malware Remover is a built-in utility designed to protect QNAP devices against harmful software. Malware programs are often disguised as or embedded in nonmalicious files and software. They often attempt to gain access to sensitive user information and may negatively impact device performance.

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.

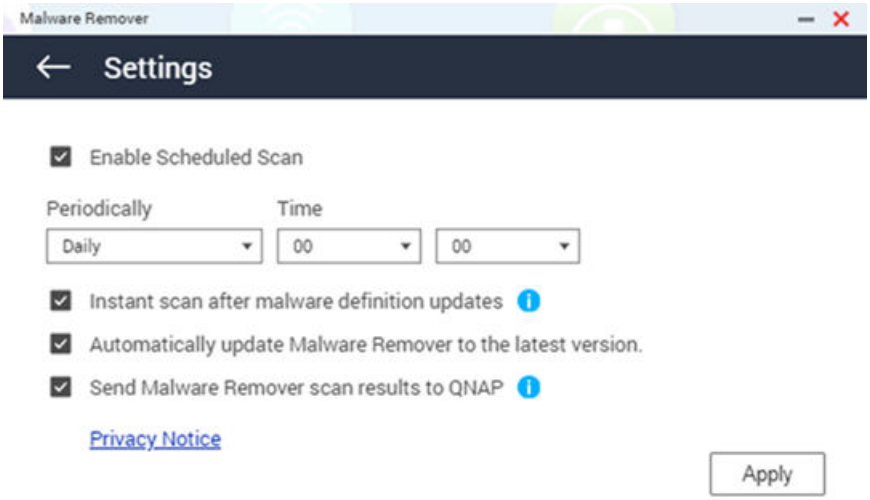
1. Open Malware Remover.
2. Click .
3. Choose from the scheduled scan drop-down menu to configure the settings.

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**.

Settings

This screen contains the Malware Remover configuration options.



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 the following data: • NAS model • NAS IP address (The IP address is immediately deleted after analyzing the malware scan results.) • Scan status • Scan errors • Malware detection date and time • Malware ID **Note** Disabling this option prevents Malware Remover from sending any data to QNAP.

4. Click **Apply**.
   Malware Remover saves the settings.

18. 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 NAS, 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.
NAS User Manual	View or download QNAP NAS user manuals.
Help Center	Find how to use a QNAP NAS.
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.

19. Console Management

Console Management is a text-based tool that helps the admin account 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 the admin account can use Console Management, and it is automatically launched when the admin account logs 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 the admin account.
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 the admin account.

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 admin@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 the admin account.
   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.
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.
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.

Option	User Action
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 the admin account, 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 the admin account, 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.
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 the admin account, 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 the admin account, 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.