



QNAP

QuTS hero h5.0.x

User Guide

Contents

1. Overview

About QuTS hero.....	11
What's New in QuTS hero.....	12
Support and Other Resources.....	13
NAS Access.....	13
Accessing the NAS Using a Browser.....	14
Accessing the NAS Using Qfinder Pro.....	14
Accessing the NAS Using Qmanager.....	15
2-step Verification.....	15
QuTS hero Navigation.....	17
Task Bar.....	17
Main Menu.....	25
Desktop.....	27

2. Getting Started

Storing Data.....	32
Accessing Data.....	32
Backing Up Data.....	33
Configuring Privilege Settings.....	33
Setting Up Remote Access.....	34
Acquiring Apps and Licenses.....	34
Securing the NAS.....	35

3. System Settings

General Settings.....	37
Configuring System Administration Settings.....	37
Configuring Time Settings.....	39
Configuring Daylight Saving Time.....	40
Configuring Codepage Settings.....	40
Configuring Region Settings.....	41
Configuring the Login Screen.....	41
Configuring Console Management.....	41
Security.....	42
Configuring the Allow/Deny List.....	42
Configuring IP Access Protection.....	43
Configuring Account Access Protection.....	43
SSL Certificate & Private Key.....	43
Configuring the Password Policy.....	45
Hardware.....	46
Configuring General Hardware Settings.....	46
Configuring Audio Alert Settings.....	47
Configuring the Backup Battery Unit (BBU) Settings.....	47
Configuring Smart Fan Settings.....	48
Configuring Hardware Resource Settings.....	48
Viewing SR-IOV Device Settings.....	49
Power.....	50
EuP Mode.....	50
Wake-on-LAN (WOL).....	50
Power Recovery.....	51
Power Schedule.....	51
Firmware Update.....	52

Firmware Update Requirements.....	52
Checking for Live Updates.....	53
Updating the Firmware Automatically.....	53
Updating the Firmware Manually.....	54
Updating the Firmware Using Qfinder Pro.....	55
Backup/Restore.....	56
Backing Up System Settings.....	56
Restoring System Settings.....	57
System Reset and Restore to Factory Default.....	57
External Device.....	59
Uninterruptible Power Supply (UPS).....	59
System Status.....	61
Resource Monitor.....	62

4. Privilege Settings

Users.....	63
Default Administrator Account.....	63
Creating a Local User.....	65
Creating Multiple Users.....	67
User Account Lists.....	68
Importing Users.....	69
Exporting Users.....	70
Modifying User Account Information.....	71
Deleting Users.....	73
Home Folders.....	73
User Groups.....	74
Default User Groups.....	74
Creating a User Group.....	74
Modifying User Group Information.....	75
Deleting User Groups.....	76
Shared Folders.....	76
Default Shared Folders.....	76
Creating a Shared Folder.....	77
Editing Shared Folder Properties.....	82
Refreshing a Shared Folder.....	84
Removing Shared Folders.....	84
ISO Shared Folders.....	84
Shared Folder Permissions.....	86
Folder Aggregation.....	89
Shared Folder Encryption.....	92
Shared Folder Access.....	93
Quota.....	98
Enabling Quotas.....	99
Editing Quota Settings.....	99
Exporting Quota Settings.....	100
Quota Conflicts.....	100
Domain Security.....	100
Active Directory (AD) Authentication.....	101
Azure Active Directory Single Sign-On (SSO).....	104
LDAP Authentication.....	105
AD and LDAP Management.....	107
Domain Controller.....	108
Enabling a Domain Controller.....	109
Resetting a Domain Controller.....	110
Default Domain User Accounts.....	110
Creating a Domain User.....	110
Creating Multiple Domain Users.....	111

Domain User Account Lists..... 112
 Modifying Domain User Account Information..... 114
 Deleting Domain Users..... 115
 Domain User Groups..... 116
 Computers..... 117
 DNS..... 119
 Back Up/Restore..... 121

5. Services

Antivirus..... 123
 Enabling Antivirus..... 123
 Scanning Shared Folders..... 123
 Managing Scan Jobs..... 125
 Managing Reported Scan Jobs..... 125
 Managing Quarantined Files..... 126
 Servers..... 127
 Web Server..... 127
 Enabling the LDAP Server..... 130
 MariaDB Server..... 130
 Syslog Server..... 136
 RADIUS Server..... 139
 Enabling the TFTP Server..... 141
 Enabling the NTP Server..... 142

6. File Station

Overview..... 143
 About File Station..... 143
 System Requirements..... 143
 Supported File Formats..... 143
 Parts of the User Interface..... 144
 Settings..... 146
 File Operations..... 149
 Uploading a File..... 150
 Downloading a File..... 151
 Opening a File..... 151
 Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension..... 152
 Opening a Text File Using Text Editor..... 152
 Viewing a File in Google Docs..... 153
 Viewing a File in Microsoft Office Online..... 153
 Opening Image Files Using Image2PDF..... 154
 Viewing File Properties..... 154
 Modifying File Permissions..... 155
 Sorting Files..... 156
 Copying a File..... 156
 Moving a File..... 157
 Renaming a File..... 158
 Deleting a File..... 159
 Restoring a Deleted File..... 159
 Mounting an ISO File..... 160
 Unmounting an ISO File..... 160
 Compressing a File..... 160
 Sharing a File or Folder by Email..... 161
 Sharing a File or Folder on a Social Network..... 164
 Sharing a File or Folder Using Share Links..... 165
 Sharing a File or Folder with a NAS User..... 167
 Playing an Audio File..... 169

Playing a Video File.....	169
Playing a Video File Using CAYIN MediaSign Player.....	170
Opening a 360-degree Image or Video File.....	170
Streaming to a Network Media Player.....	171
Adding a File to the Transcoding Folder.....	171
Canceling or Deleting Transcoding.....	172
Viewing Transcode Information.....	173
Extracting Compressed Files or Folders.....	173
Folder Operations.....	174
Uploading a Folder.....	174
Uploading a Folder Using Drag and Drop.....	175
Viewing Folder Properties.....	175
Viewing Storage Information.....	176
Modifying Folder Permissions.....	177
Viewing Qsync Folders.....	178
Managing Share Links.....	178
Viewing Files and Folders Shared with Me.....	179
Creating a Folder.....	179
Copying a Folder.....	179
Creating a Desktop Shortcut.....	180
Adding a Folder to Favorites.....	180
Removing a Folder from Favorites.....	181
Compressing a Folder.....	181
Deleting a Folder.....	182
Creating a Shared Folder.....	183
Sharing Space with a New User.....	188
Adding a Folder to the Transcoding Folder.....	189
Canceling or Deleting Transcoding.....	189
Locking or Unlocking an Encrypted Shared Folder.....	190
Keeping a Folder or a File in Reserved Cache.....	191
Removing a Folder from Reserved Cache.....	192

7. Storage & Snapshots

QNAP Flexible Storage Architecture.....	193
Global Settings.....	194
Storage Global Settings.....	194
Disk Health Global Settings.....	194
Snapshot Global Settings.....	195
Storage.....	196
Disks.....	196
Storage Pools.....	202
Shared Folders.....	211
RAID.....	221
Self-Encrypting Drives (SEDs).....	226
Expansion Units.....	229
Expansion Unit Actions.....	229
Expansion Unit Recovery.....	229
QNAP External RAID Devices.....	230
QNAP JBOD Enclosures.....	238
Snapshots.....	240
Snapshot Storage Limitations.....	240
Snapshot Creation.....	240
Snapshot Management.....	242
Snapshot Data Recovery.....	244
Snapshot Clone.....	247
Snapshot Replica.....	248
Cache Acceleration.....	259

- Cache Acceleration Requirements..... 259
- Creating the SSD Cache..... 259
- Configuring SSD Cache Disks..... 261
- Configuring Cached Storage..... 262
- Removing the SSD Cache..... 262
- External Storage..... 263
- External Storage Device Actions..... 263
- External Storage Disk Actions..... 263
- External Storage Partition Actions..... 263
- Formatting an External Storage Disk or Partition..... 263
- Remote Disk..... 265
- Remote Disk Limitations..... 265
- Adding a Remote Disk..... 265
- Remote Disk Actions..... 267
- VJBOD (Virtual JBOD)..... 267
- VJBOD Requirements..... 267
- VJBOD Limitations..... 268
- VJBOD Automatic Reconnection..... 268
- VJBOD Creation..... 268
- VJBOD Management..... 272
- VJBOD Cloud..... 275
- Installing VJBOD Cloud..... 275
- VJBOD Cloud Volume and LUN Creation..... 275
- VJBOD Cloud Management..... 288
- Transfer Resources..... 290
- Event Logs..... 292
- Licenses..... 292
- SnapSync..... 293
- SnapSync Requirements..... 293
- SnapSync Restrictions..... 294
- SnapSync Job Creation..... 294
- SnapSync Management..... 299
- SnapSync Performance Test..... 302

8. iSCSI & Fibre Channel

- Storage Limits..... 304
- iSCSI Storage Limits..... 304
- Fibre Channel Storage Limits..... 304
- iSCSI & Fibre Channel Global Settings..... 304
- LUNs..... 304
- Creating a Block-Based LUN..... 305
- LUN Import/Export..... 307
- iSCSI..... 310
- Getting Started with iSCSI..... 310
- iSCSI Performance Optimization..... 310
- iSCSI Targets..... 311
- iSCSI LUN Management..... 314
- iSCSI Access Control List..... 316
- iSCSI Target Authorization..... 318
- QNAP Snapshot Agent..... 319
- Fibre Channel..... 320
- Fibre Channel Ports..... 320
- Fibre Channel Storage..... 323
- Fibre Channel WWPN Aliases..... 324

9. ZFS Pool Profiling Tool

Installing ZFS Pool Profiling Tool.....	328
Storage Pool Over-Provisioning.....	328
Creating a Storage Pool Over-Provisioning Test.....	328
Test Reports.....	329
Settings.....	330

10. Network & Virtual Switch

About Network & Virtual Switch.....	331
Parts of the User Interface.....	331
Basic Network Adapter Configuration.....	332
Configuring IPv4 Settings.....	333
Configuring IPv6 Settings.....	334
Configuring the System Default Gateway.....	336
Configuring Static Route Settings.....	338
IP Addressing Services Configuration.....	341
Configuring DNS Server Settings.....	341
Configuring DHCP Server Settings	342
Adding DHCP Clients to a DHCP Server.....	349
Configuring RADVD Server Settings.....	350
Configuring DDNS Service Settings.....	356
LAN Switching Configuration.....	357
Configuring VLAN Settings.....	357
Configuring Port Trunking Settings.....	358
Virtual Switch Configuration.....	364
Creating a Virtual Switch in Basic Mode.....	364
Creating a Virtual Switch in Advanced Mode.....	368
Creating a Virtual Switch in Software-defined Switch Mode.....	380
Network Policies Configuration.....	383
Configuring Forward Error Correction (FEC) Settings.....	383
Wireless Network Configuration.....	384
Adding a Wireless Network.....	384
Enabling Wi-Fi.....	387
Connecting to a Wireless Network	387
Understanding the Wireless Connection Messages.....	396
Accessing the Wireless Access Point (AP) Settings.....	397
USB QuickAccess Configuration.....	397
Enabling USB QuickAccess	398
Configuring the USB QuickAccess IP address	398
Configuring USB QuickAccess Authentication	399
Thunderbolt Interface Configuration.....	399
Enabling T2E with Qfinder Pro.....	400
Enabling T2E on macOS.....	400

11. Network & File Services

About Network & File Services.....	401
QNAP Service Ports.....	401
Configuring Network Access Settings.....	402
Configuring Service Binding Settings	403
Configuring Proxy Server Settings.....	403
Configuring Reverse Proxy Rule Settings.....	404
Modifying Reverse Proxy Rules.....	405
Configuring Network Protocol Settings.....	406
Configuring Telnet Connections.....	406
Configuring SSH Connections.....	407
Editing SSH Access Permissions.....	407
Configuring SNMP Settings.....	408

- Downloading the SNMP MIB..... 409
- Configuring File Sharing Protocol Settings..... 410
 - Configuring Samba (Microsoft Networking) Settings..... 410
 - Configuring AFP (Apple Networking) Settings..... 412
 - Configuring NFS Service Settings..... 413
 - Accessing FTP (QuFTP Service) Settings..... 414
 - Configuring WebDAV Settings..... 414
- Enabling Service Discovery Settings..... 417
 - Enabling the UPnP Discovery Service..... 417
 - Enabling the Bonjour Discovery Service..... 417
- Network Recycle Bin Management..... 417
 - Configuring the Network Recycle Bin..... 417
 - Deleting All Files in the Network Recycle Bin..... 418
 - Restricting Access to the Network Recycle Bin..... 418

12. myQNAPcloud

- Getting Started..... 419
- Account Setup..... 419
 - Creating a QNAP ID With Email or Phone Number..... 419
 - Registering a Device to myQNAPcloud..... 420
 - Installing myQNAPcloud Link..... 423
- Overview..... 423
- Configuring UPnP Port Forwarding..... 424
- Configuring DDNS Settings..... 425
- Restarting DDNS Service..... 425
- Configuring Published Services..... 426
- Enabling myQNAPcloud Link..... 426
- Configuring Device Access Controls..... 427
- Installing an SSL Certificate..... 427

13. App Center

- Navigation..... 429
 - Left Panel..... 429
 - Toolbar..... 429
 - Main Area..... 430
- App Management..... 431
 - Viewing App Information..... 431
 - Installing an App from App Center..... 432
 - Installing an App Manually..... 432
 - Updating an App..... 433
 - Batch Updating Multiple Apps..... 433
 - Enabling or Disabling an App..... 434
 - Migrating an App..... 434
 - Granting or Denying User Access to an App..... 434
 - Uninstalling an App..... 435
- App Center Settings..... 435
 - Adding an App Repository..... 435
 - Configuring App Update Settings..... 436
 - Digital Signatures..... 436
 - Enabling Installation of Apps without Digital Signatures..... 437

14. Licenses

- About QNAP Licenses..... 438
 - License Types and Plans..... 438
 - Validity Period..... 438
- License Portals and Utility..... 439

Software Store.....	439
License Center.....	439
License Manager.....	439
Buying a License Using QNAP ID.....	440
License Activation.....	441
Activating a License Using QNAP ID.....	441
Activating a License Using a License Key.....	443
Activating a License Using a Product Key or PAK.....	444
Activating a License Offline.....	445
License Deactivation.....	446
Deactivating a License Using QNAP ID.....	446
Deactivating a License Offline.....	447
License Extension.....	448
Extending a License Using QNAP ID.....	448
Extending a License Offline Using an Unused License.....	450
Extending a License Offline Using a Product Key.....	452
Upgrading a License.....	453
Viewing License Information.....	454
Recovering Licenses.....	455
Transferring a License to the New QNAP License Server.....	457
Deleting a License.....	457

15. Multimedia

HybridDesk Station (HD Station).....	459
Installing HD Station.....	460
Configuring HD Station.....	460
HD Station Applications.....	461
Using HD Player in HD Station.....	461
DLNA Media Server.....	462
Enabling DLNA Media Server.....	462
Configuring DLNA Media Server.....	462
Media Streaming Add-on.....	463
Configuring General Settings.....	463
Configuring Browsing Settings.....	464
Configuring Media Receivers.....	465
Multimedia Console.....	465
Overview.....	465
Content Management.....	466
Indexing.....	467
Thumbnail Generation.....	468
Transcoding.....	470
Multimedia App Suite.....	475

16. QuLog Center

Monitoring System Logs.....	478
System Event Log.....	478
System Access Logs.....	478
Local Logs.....	479
Local System Event Logs.....	479
Local System Access Logs.....	482
Online Users.....	484
Creating a Custom Filter Tab for Local Device System Logs.....	485
Local Log Settings.....	488
QuLog Service.....	492
Configuring Log Sender Settings.....	492
Configuring Log Reciever Settings.....	494

Viewing and Managing Remote Logs.....497

Notification Settings.....505

 Configuring Notification Rule Settings.....505

 Adding a Log Filter.....506

 Editing a Log Filter.....507

 Removing a Log Filter.....507

17. Notification Center

About Notification Center.....509

Parts of the User Interface.....509

Managing Notification Queue and History.....510

Service Account and Device Pairing.....511

 Email Notifications.....511

 SMS Notifications.....513

 Instant Messaging Notifications.....515

 Push Notifications.....517

System Notification Rules.....518

 Managing Event Notification Rules.....518

 Creating an Event Notification Rule.....519

 Managing Alert Notification Rules.....522

 Creating an Alert Notification Rule.....522

Settings.....525

 Enabling Send Notification Data to QNAP.....525

 Disabling Send Notification Data to QNAP.....525

Global Notification Settings.....526

System Event Logs.....526

18. Malware Remover

About Malware Remover.....528

Overview.....528

Running a Malware Scan.....528

Running a Scheduled Scan.....529

Configuring Malware Remover.....529

19. Helpdesk

Overview.....531

 Configuring Settings.....531

Help Request.....531

 Submitting a Ticket.....532

Remote Support.....533

 Enabling Remote Support.....533

 Extending Remote Support.....533

 Disabling Remote Support.....533

Diagnostic Tool.....534

 Downloading Logs.....534

 Performing an HDD Standby Test.....534

 Performing an HDD Stress Test.....534

20. Console Management

Enabling Secure Shell (SSH).....535

 Enabling SSH on the NAS.....535

 Enabling SSH on the NAS Using Qfinder Pro.....535

Accessing Console Management.....535

 Accessing Console Management from Windows.....535

 Accessing Console Management from Mac.....536

Logging In to Console Management.....536

Managing Existing Applications.....	536
Activating or Deactivating a License.....	537
Sorting and Filtering System Logs.....	538
Showing Network Settings.....	540
Restoring or Reinitializing the Device.....	540
Rebooting the NAS.....	540
Rebooting the Device Into Rescue Mode.....	540
Rebooting the Device Into Maintenance Mode.....	541

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	Major New Features
QuTS hero h5.0.0	<ul style="list-style-type: none"> • QuTS hero administrators can now purchase and activate app licenses in the App Center. • QuTS hero now supports Desktop Notice Board, which provides notifications for various events and announcements. • QuTS hero now supports creating instant clones for snapshots, which allow users to instantly clone shared folders from snapshots. • QuTS hero now supports TLS 1.3 for HTTPS secure connection. • QuTS hero now enables dynamic wallpapers by default. • Users can now use exFAT without purchasing an exFAT license. • Users can now use port 443 for Let's Encrypt domain validation challenges. • Users can now configure reverse proxy rules to hide the sensitive information on the server from clients and to enhance the security of data transmission over the network. • Users can now import custom root certificates to certify the SSL certificate of a server that the NAS needs to access. • Users in the administrator group now have read/write access permissions for default shared folders, except the "homes" shared folder. • Users can now set scrubbing schedules more flexibly to reduce impact on system performance. • Added an option to choose whether to redirect users to the NAS login screen when connecting to the NAS IP address without the system port. To enhance device security, this option is disabled by default. • To enhance device security, UPnP Discovery Service is now disabled by default. • Added the option to enable strong cipher suites. • To ensure device security, QuTS hero now reminds users to disable the default "admin" account and to create another administrator account during HDMI Installation. • To enhance system security, users are now required to create a new administrator account to replace the "admin" account during HDMI Installation. • Added support for Forward Error Correction (FEC) for error detection and error correction in data transmission over unreliable or noisy communication channels. • Replaced SQL Server with MariaDB 5/MariaDB 10, which can be installed in the App Center. • Shortened the default interval of automatic synchronization with the time server from 7 days to 1 day. • Improved the user interface of Advanced Search in QuLog Center.

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

NAS Access

Method	Description	Requirements
Web browser	<p>You can access the NAS using any computer on the same network if you have the following information:</p> <ul style="list-style-type: none"> NAS name (Example: http://example123/) or IP address Logon credentials of a valid user account <p>For details, see Accessing the NAS Using a Browser.</p>	<ul style="list-style-type: none"> Computer that is connected to the same network as the NAS Web browser
Qfinder Pro	<p>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.</p> <p>For details, see Accessing the NAS Using Qfinder Pro.</p>	<ul style="list-style-type: none"> Computer that is connected to the same network as the NAS Web browser Qfinder Pro
Qmanager	<p>Qmanager is a mobile application that enables administrators to manage and monitor NAS devices on the same network.</p> <p>You can download Qmanager from the Apple App Store and the Google Play Store.</p> <p>For details, see Accessing the NAS Using Qmanager.</p>	<ul style="list-style-type: none"> Mobile device that is connected to the same network as the NAS Qmanager

Method	Description	Requirements
Explorer (Windows)	You can map a NAS shared folder as a network drive to easily access files using Explorer. For details, see the following topics. <ul style="list-style-type: none"> • Mapping a Shared Folder on a Windows Computer • Mounting a Shared Folder using WebDAV on Windows 	<ul style="list-style-type: none"> • Windows computer that is connected to the same network as the NAS • Qfinder Pro
Finder (macOS)	You can mount a NAS shared folder as a network drive to easily access files using Finder. For details, see the following topics. <ul style="list-style-type: none"> • Mounting a Shared Folder on a Mac Computer • Mounting a Shared Folder Using WebDAV on Mac 	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Tap Add NAS manually. b. Specify the following information. <ul style="list-style-type: none"> • Host name or IP address of the NAS • Password of the admin account c. Tap Save.
Sign in using QID	<ol style="list-style-type: none"> a. Tap Sign in QID. b. Specify the following information. <ul style="list-style-type: none"> • 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> Go to Control Panel > Privilege > Users. Identify a locked out user, and then click . Deselect 2-step Verification. Click OK.
An administrator is locked out and no other administrators can access the account.	An administrator must restore the factory settings.	<p>Press the RESET button on the back of the NAS for three seconds. The NAS restores the default administrator password and network settings.</p> <p>Note For information on the default admin password, see Backup/Restore.</p> <p>Warning Pressing the RESET button for 10 seconds resets all settings and deletes all data on the NAS.</p>



QuTS hero Navigation



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

Task Bar



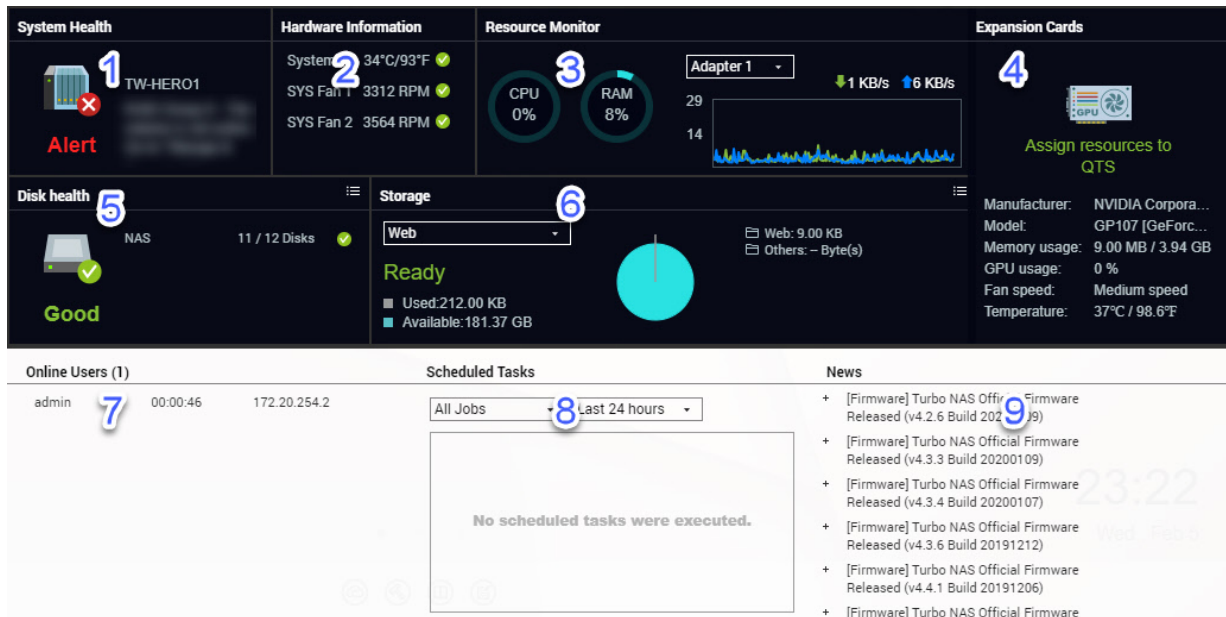
No.	Element	Possible User Actions
1	Show Desktop	Click the button to minimize or restore all open windows.
2	Main Menu	Click the button to open the Main Menu panel on the left side of the desktop.
3	Search	<ul style="list-style-type: none"> Type key words to locate settings, applications, and help content. Click an entry in the search results to open the application, system utility, or Help Center window. <p>Tip App or utility search results are classified into Systems, Application, and Help.</p>

No.	Element	Possible User Actions
4	<p>Volume Control</p> <p> Important This feature is only available on models with certain hardware specifications.</p>	<p>Click the button to view the following:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • HD Station • Music Station • OceanKTV • Audio Alert Volume: Click and drag the slider thumb to adjust the volume of system audio alerts.
5	<p>Background Tasks</p>	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Task name • Task description • Progress (percentage of completion) • Click  to stop a task.
6	<p>External Devices</p>	<ul style="list-style-type: none"> • 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	<p>Event Notifications</p>	<ul style="list-style-type: none"> • Hover the mouse pointer over the button to see the number of recent errors and warnings. • Click the button to view the following details for each event: <ul style="list-style-type: none"> • 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	<p>Options</p>	<p>Click your profile picture to open the Options screen.</p>

No.	Element	Possible User Actions
9	[USER_NAME]	<p>Click the button to view the last login time and the following menu items:</p> <ul style="list-style-type: none"> • Options: Opens the Options window • Sleep: Keeps the NAS powered on but significantly reduces power consumption <p> Note This feature is only available on models with certain hardware specifications.</p> <ul style="list-style-type: none"> • Restart: Restarts the NAS • Shutdown: Shuts down QuTS hero and then powers off the NAS <p> Tip You can also power off the NAS using one of the following methods:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Logout: Logs the user out of the current session

No.	Element	Possible User Actions
10	More	<p>Click the button to view the following menu items:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Operating system • Hardware model • Operating system version • Number of installed drives • Number of empty drive bays • System pool name • Used disk space • Available disk space
11	Notice Board	Display all system notifications and getting started guide during initialization.
12	Dashboard	Click the button to display the dashboard.

Dashboard




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




Tip

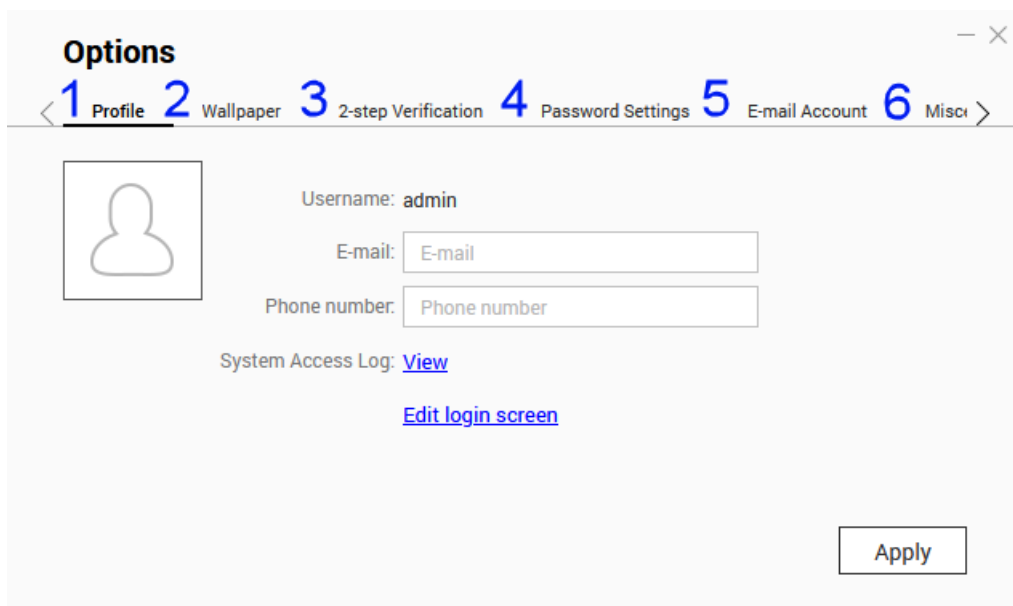
You can click and drag a section onto any area of the desktop.


No.	Section	Displayed Information	User Actions
1	System Health	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Number of installed disks • Health status of installed disks • Number of VJBOD disks • Health status of VJBOD disks 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Capacity/size • Temperature • Health status • Click Details to open Storage & Snapshots > Overview .

No.	Section	Displayed Information	User Actions
6	Storage	<p>For each shared folder:</p> <ul style="list-style-type: none"> • Status • Used space • Available space • Folder size <p>For each storage pool:</p> <ul style="list-style-type: none"> • Status • Used space • Available space • Shared folder size <p>For each LUN:</p> <ul style="list-style-type: none"> • Status • Used space • Available space 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Username • IP address • Total connection time • Connection type 	<p>Click the heading to open Control Panel > System > QuLog Center > Online Users .</p>

Options




No.	Tab	Possible User Actions
1	Profile	<ul style="list-style-type: none"> • Specify the following optional information: <ul style="list-style-type: none"> • Profile picture • Email address • Phone number • Click View to display the System Access Log screen. • Click Edit login screen to open the Login Screen configuration screen in the Control Panel window. • Click Apply to save all changes.
2	Wallpaper	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Note The nighttime mode dynamic wallpaper is set as the default wallpaper.</p> </div> </div> <ul style="list-style-type: none"> • Perform any of the following actions: <ul style="list-style-type: none"> • Dynamic wallpaper: Specify the daytime and nighttime, then select a wallpaper pairing. The system automatically switches the wallpaper between daytime and nighttime modes at the specified time. • Picture: Select from the default images or upload an image, then specify the image fill mode. • Color: Select a color from the default settings or specify a color. • Click Apply to save all changes.
3	2-step Verification	Click Get Started to open the configuration wizard. For details, see Enabling 2-step Verification .
4	Change Password	<ul style="list-style-type: none"> • Specify the following information to change your password. <ul style="list-style-type: none"> • Old password • New password: Specify a password with a maximum of 64 characters. QNAP recommends using passwords with at least 6 characters. • Specify an email address to receive a notification email to recover your password if you forgot the password. You need to configure SMTP settings in Notification Center to use this feature. • Click Apply to save all changes.
5	E-mail Account	<ul style="list-style-type: none"> • Add, edit, and delete email accounts to use when sharing files. • Click Apply to save all changes.

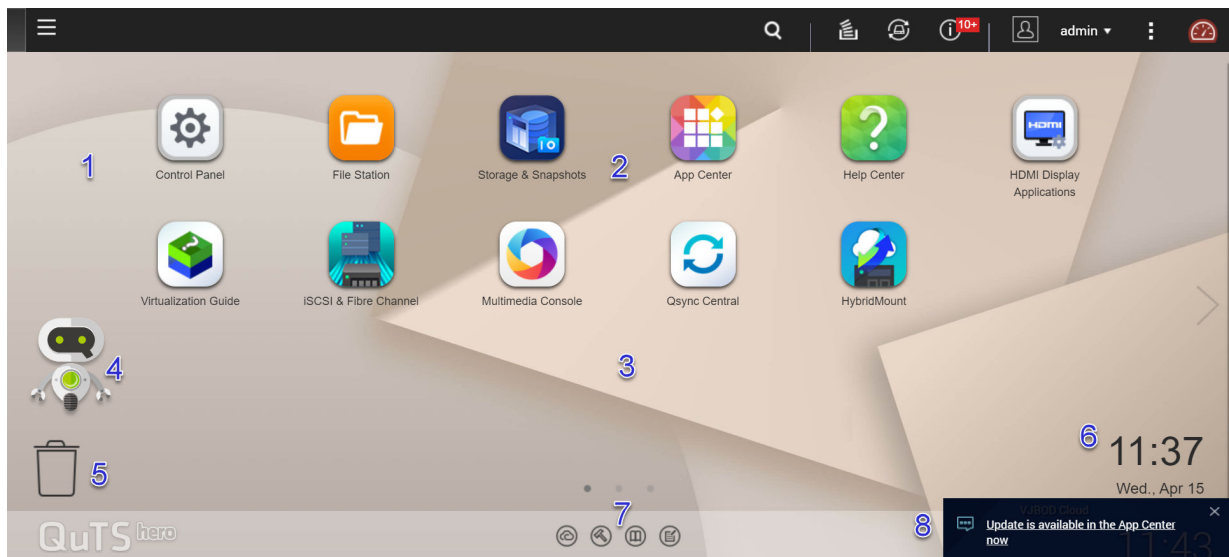
No.	Tab	Possible User Actions
6	Miscellaneous	<ul style="list-style-type: none"> • Enable the following settings as necessary. <ul style="list-style-type: none"> • Auto logout after an idle period: Specify the duration of inactivity after which the user is automatically logged out. • Warn me when leaving QuTS Hero: When enabled, QuTS hero prompts users for confirmation whenever they try to leave the desktop (by clicking the Back button or closing the browser). QNAP recommends enabling this setting. • Reopen windows when logging back into NAS: When enabled, the current desktop settings (including all open windows) are retained until the next session. • Show the desktop switching button: When enabled, QuTS hero displays the desktop switching buttons < > on the left and right sides of the desktop. • Show the link bar on the desktop: When enabled, QuTS hero displays the link bar on the bottom of the desktop. • Show the Dashboard button: When enabled, QuTS hero displays the button to show the dashboard on the taskbar. • Show the NAS time on the desktop: When enabled, QuTS hero displays the current NAS time, day, and date at the bottom-right of the desktop. • Keep Main Menu open after selection: When enabled, QuTS hero keeps the main menu pinned to the desktop after you open it. • Show a list of actions when external storage devices are detected: When enabled, QuTS hero displays an Autoplay dialog box whenever an external storage device is inserted into a USB or SATA port. • Click Apply to save all changes.





Main Menu








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

No.	Section	Description	Possible User Actions
2	System	<p>Displays a list of system utilities and other programs that enable you to manage the NAS. The following are the default system utilities:</p> <ul style="list-style-type: none"> • Control Panel • Storage & Snapshots • iSCSI & Fibre Channel • Users • Network & Virtual Switch • myQNAPcloud • Resource Monitor • App Center • Help Center • Qboost • HDMI Display Applications <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note This menu item only appears on models with certain hardware specifications.</p> </div>	<ul style="list-style-type: none"> • Open a system utility or application in the QuTS hero desktop <ul style="list-style-type: none"> • 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) <ul style="list-style-type: none"> • Right-click a menu item and then select Open in new browser tab. • Create a shortcut on the desktop <ul style="list-style-type: none"> • Right-click a menu item and then select Create shortcut. • Click and drag a menu item to the desktop.
3	Applications	<p>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:</p> <ul style="list-style-type: none"> • File Station • Helpdesk • License Center • Multimedia Console • Notification Center • QuTS hero SSL Certificate 	
4	Search	Displays apps that meet your search criteria.	Enter keywords.

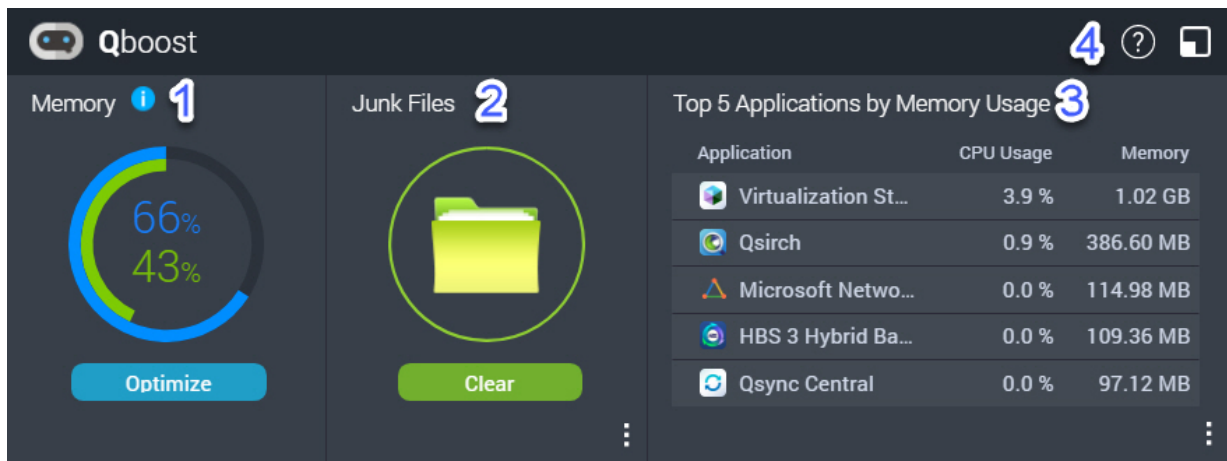
Desktop





#	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: <ul style="list-style-type: none"> Control Panel File Station Storage & Snapshots App Center Help Center 	<ul style="list-style-type: none"> Click an icon to open the application window. Right-click an icon and then select one of the following: <ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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	<p>This displays the list of files that the currently active user moved to the Recycle Bin.</p> <p>The following applications provide users a choice between permanently deleting files and moving files to the Recycle Bin.</p> <ul style="list-style-type: none"> • File Station • Music Station • Photo Station • Video Station 	<ul style="list-style-type: none"> • Click  to open the Recycle Bin screen in the File Station window. • Right-click  and then select one of the following: <ul style="list-style-type: none"> • 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.	<p>Click any of the following buttons:</p> <ul style="list-style-type: none"> • : 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	<p>This notifies the user about important system events that may or may not require user action. When there is more than one group of notifications, the notices will be arranged according to the notification type on a notice board. You can also view notifications in Notifications Board.</p> <p> Note When you initialize QuTS hero, the Getting Started guide will appear in notifications after installation.</p>	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. You can download the utility from App Center. It provides the following information:

#	Section	Description	User Actions
1	Memory	<p>A graphic showing memory usage on the NAS.</p> <ul style="list-style-type: none"> 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. 	<p>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.</p>
2	Junk Files	<p>Junk files are unnecessary system files and files in the Recycle Bin, which consume disk space and memory.</p>	<ul style="list-style-type: none"> 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	<p>Top five applications and services that consume the most memory</p>	<p>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.</p>



#	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: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Click  to change the status to Always Enabled. • Click  to change the status to Always Disabled.

Objective	Action
<p>Create a schedule for enabling and disabling an application or service.</p>	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Warning Setting a schedule may force an application to stop in the middle of a task.</p> </div> </div> <ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Click Apply: Applies the schedule to the selected application or service • Select Auto-apply: Applies the schedule to all applications and services
<p>Delete a schedule.</p>	<p>Click  to delete the schedule and disable an application or service.</p>
<p>Remove an application.</p>	<p>Click . This function applies only to applications that are available in App Center.</p>

2. Getting Started

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

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

Storing Data

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

1. Create a storage pool.

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

For details, see [Creating a Storage Pool](#).

2. Create a shared folder.

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



Tip

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

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

Accessing Data

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

- Access files via File Station.
 - a. Access the NAS.

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

For details, see:

 - [Accessing the NAS Using a Browser](#)
 - [Accessing the NAS Using Qfinder Pro](#)
 - b. Open File Station.

File Station is the file manager in QuTS hero, allowing you to browse, manage, and share files on the NAS. You can also create and configure shared folders in File Station to facilitate file management.

For details, see [File Station](#).

- Access files via shared folders mounted on your computer.
You can mount a shared folder as a network drive on your computer. This allows you to directly access mounted shared folders using the file manager on your Windows or macOS computer.
For details, see:
 - [Mapping a Shared Folder on a Windows Computer](#)
 - [Mounting a Shared Folder on a Mac Computer](#)

Backing Up Data

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

Hybrid Backup Sync allows you to back up, restore, and synchronize data between your local NAS and multiple destinations, including a remote NAS, external devices, cloud storage services. You can also take snapshots for shared folders on your local NAS and use Snapshot Replica to back up these snapshots to another storage pool or remote NAS.

- Use Hybrid Backup Sync to back up your NAS data.
 - a. Install Hybrid Backup Sync on the NAS.
 - b. Create a backup job or a sync job.

Hybrid Backup Sync is a comprehensive solution for data backup and disaster recovery. In addition to data deduplication and encryption, this essential tool also provides various features to facilitate job configuration and management.

For details, see [Hybrid Backup Sync Help](#).

- Take and back up snapshots for your NAS data.
 - a. Take snapshots for shared folders.
 - b. Back up snapshots with Snapshot Replica.

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

For details, see:

- [Taking a Snapshot](#)
- [Creating a Snapshot Replica Job](#)

Configuring Privilege Settings

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

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

1. Create an administrator account.
You can create a new user account to replace the admin account. To grant administrator privileges to this new user, you must add this new user to the administrator group. You should also grant shared folder access permissions to this user.
For details, see [Creating an Administrator Account](#).
2. Disable the admin account.
After creating a new administrator, you should disable the default admin account and then start managing the NAS with this new administrator account.
For details, see [Disabling a Default Administrator Account](#).
3. Create more users or user groups.
You can create other users or user groups and grant them different levels of privileges to control access to your data on the NAS.
For details, see:
 - [Creating a Local User](#)
 - [Creating a User Group](#)

Setting Up Remote Access

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

1. Create a QNAP ID.
QNAP ID is your QNAP account that allows you to access various QNAP services. To create a QNAP ID, go to <https://account.qnap.com/>.
For details, see [Creating a QNAP ID With Email or Phone Number](#).
2. Register the NAS to your QNAP ID.
After creating a QNAP ID, you need to enable the myQNAPcloud service on your NAS and then associate your device with your QNAP ID. You can also configure various remote access settings in myQNAPcloud.
For details, see [Registering a Device to myQNAPcloud](#).
3. Remotely access the NAS via myQNAPcloud.
After setting up myQNAPcloud on your NAS, you can remotely access and manage the NAS via the [myQNAPcloud website](#) or via the SmartURL generated for your NAS.
4. Remotely access the NAS on your mobile device.
QNAP provides a wide range of mobile applications that enable you to access, manage, monitor, and back up your NAS wherever you go. After installing these QNAP applications on your mobile devices, you must sign in to them with your QNAP ID.
For details, go to <https://www.qnap.com/en/mobile-apps>.

Acquiring Apps and Licenses

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

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

For details, see [App Center](#).

2. Purchase licenses in the QNAP Software Store.
[QNAP Software Store](#) is an online store where you can purchase licenses and manage your orders. QNAP provides various types of licenses and subscription plans to meet different needs and usage environments.
 For details, see [Licenses](#).
3. Activate licenses in the License Center or License Manager.
 Some licenses are automatically activated after being purchased. However, sometimes you must manually activate a license.
 License Center allows you to manage licenses on your local device. [License Manager](#) allows you and your organization to manage licenses under your QNAP ID.
 For details, see [Licenses](#).

Securing the NAS

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

1. Prevent unauthorized access to your device.
 - a. Create a new administrator account and disable the admin account.
 The admin account is the default administrator account. Nevertheless, to enhance the security of your device, we strongly recommend creating another administrator account and then disabling the admin account.
 For details, see [Default Administrator Account](#).
 - b. Enhance user password strength.
 We recommend enhancing your password strength and changing your passwords regularly to prevent brute-force attacks.
 For details, see [Modifying User Account Information](#).
 - c. Set up 2-step verification.
 2-step verification further enhances the security of user accounts by requiring users to specify a security code in addition to their account credentials during the login process.
 For details, see [2-step Verification](#).
 - d. Remove unknown or suspicious accounts.
 We recommend verifying user accounts regularly and deleting any unknown or suspicious accounts.
 For details, see [Deleting Users](#).
 - e. Remove unnecessary permissions from general users.
 We recommend restricting the permissions of non-administrator users to limit their access to system operations and sensitive data. This helps mitigate the impact of a compromised user account.
 For details, see [Modifying User Account Information](#).
 - f. Remove unknown or suspicious applications.
 We recommend only installing applications and utilities that have digital signatures, which validate software developed by QNAP and other QNAP-trusted developers.
 You should regularly check your installed applications and remove any unknown or suspicious applications from the App Center.
 For details, see [Digital Signatures](#) and [Uninstalling an App](#).

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

 - [Configuring UPnP Port Forwarding](#)
 - [Configuring Device Access Controls](#)
 - [Configuring Published Services](#)
- 2.** Update your firmware and applications to the latest versions.

 - a.** Update the firmware to the latest version.
We strongly recommend regularly updating the firmware of your device to the latest version to benefit from the latest features, enhancements, and security fixes. You can also choose to automatically check for and install available updates.
For details, see [Firmware Update](#).
 - b.** Update applications to the latest versions.
You should regularly update your installed applications to their latest versions for better performance, functionality, and security. App Center allows you to check for all available updates and then install updates for multiple applications at the same time.
For details, see:

 - [Updating an App](#)
 - [Batch Updating Multiple Apps](#)
- 3.** Install and run security utilities on the NAS.

 - a.** Run Malware Remover.
Malware Remover is a built-in utility designed to protect QNAP devices against malicious software. You can run instant or scheduled scans to remove malicious software from your device.
For details, see [Malware Remover](#).
 - b.** Install and run Security Counselor.
Security Counselor is the security portal that allows you to centrally configure security settings and manage security components on your QNAP device. You can choose security policies, scan the device, and check for potential security weaknesses on the device. Security Counselor identifies potential risks and provides suggestions to help you enhance device security. You can also subscribe to QNAP security advisories to stay informed of the latest security fixes and solutions.


3. System Settings



General Settings



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

Configuring System Administration Settings

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

Field	User Action
Server name	<p>Specify a name containing up to 14 characters from any of the following groups:</p> <ul style="list-style-type: none"> • Letters: A to Z, a to z • Numbers: 0 to 9 • Dashes (-) <p> Important</p> <ul style="list-style-type: none"> • 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	<p>Select this option to improve transfer speeds and bandwidth utilization. This setting is enabled by default.</p> <p> Warning Enabling this option may lead to security risks.</p>
Enable secure connection (HTTPS)	<p>Select this option to allow HTTPS connections.</p> <ol style="list-style-type: none"> Select Enable secure connection (HTTPS). Select a TLS version. The default TLS version is 1.2. <p> Warning Selecting the latest TLS version may decrease compatibility for other clients in your system.</p> <ol style="list-style-type: none"> Enable strong cipher suites. Specify a port number. Select Force secure connection (HTTPS) only to require all users to connect to the NAS using only HTTPS.
Custom HTTP server header	<p>Select this option to specify a server HTTP header.</p>
Do not allow QuTS hero embedding in IFrames	<ol style="list-style-type: none"> Select this option to prevent websites from embedding QuTS hero using IFrames. Click Allowed Websites to allow a specific website to embed QuTS hero in IFrames. The Allowed Websites window appears. Click Add to add a website to the list. The Add Host Name window appears. Specify a host name. Click Add. The host name is added to the allowed websites list. Select a website, and then click Delete to delete a website from the list. Click Apply.
Enable X-Content-Type-Options HTTP header	<p>Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities.</p>
Enable Content Security Policy HTTP header	<p>Select this option to protect your device from attacks that exploit Cross Site Scripting (XSS) and data injection vulnerabilities.</p>

Field	User Action
<p>Redirect URL to NAS login page</p>	<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: flex-start;">  <div> <p>Important</p> <ul style="list-style-type: none"> 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. </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Tip</p> <p>You can check the web server settings by going to Control Panel > Applications > Web Server .</p> </div> </div> <p>Select this option to enable redirecting the URL to the NAS login page.</p> </div>

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
<p>Manual setting</p>	<p>Specify the date and time.</p>
<p>Synchronize with a time server automatically</p>	<p>Ensure that your NAS is connected to the Internet, and then specify the following information:</p> <ul style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 perform basic configurations or maintenance tasks through the text-based software tool. This feature is disabled by default.

1. Go to **Control Panel > System > General Settings > Console Management**.
2. Select **Enable Console Management**.
3. Click **Apply**.

Security

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



Configuring the Allow/Deny List



Important

If you have installed QuFirewall on your device, go to QuFirewall to configure the allow or deny list.

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

Option	Description	User Action
Allow all connections	The NAS can connect to all IP addresses and network domains.	Select Allow all connections .
Use IP deny list	The NAS cannot connect to any IP address or network domains included in the IP deny list.	<ol style="list-style-type: none"> 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. <p> Tip To remove an IP address, netmask, or IP range, select an entry from the table, and then click Remove.</p>
Use IP allow list	The NAS can only connect to the IP addresses or network domains included in the IP allow list.	<ol style="list-style-type: none"> 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. <p> Tip To remove an IP address, netmask, or IP range, select an entry from the table, and then click Remove.</p>

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

Secure Sockets Layer (SSL) is a protocol used for secure data transfers and encrypted communication between web servers and browsers. To avoid receiving alerts or error messages when accessing the web interface, upload a Secure Sockets Layer (SSL) certificate from a trusted provider through Server Certificate or import a custom root certificate to your QNAP device. QNAP recommends you purchase a valid SSL certificate from myQNAPcloud SSL Web Service Certificate. For details, see [myQNAPcloud website](#).


Replacing the Server Certificate




Warning

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

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

Option	Description
Import certificate	This option allows you to import an SSL certificate and private key from your computer.
Get from Let's Encrypt	<p>This option uses the Let's Encrypt service to validate and issue a certificate for your specified domain.</p> <div style="border-left: 2px solid #007bff; padding-left: 10px; margin-top: 10px;">  <p>Note QNAP recommends you use port 80 or 443 for authorizing the SSL certificate domain and accessing the Internet.</p> </div>
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	<ol style="list-style-type: none"> a. Click Browse to upload a valid certificate. b. Optional: Click Browse to upload an intermediate certificate.
Get from Let's Encrypt	<ol style="list-style-type: none"> 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. <div style="border-left: 2px solid #ffc107; padding-left: 10px; margin-top: 10px;">  <p>Tip Use "," to separate multiple aliases. Example: 123.web.com, 789.web.com</p> </div>
Create self-signed certificate	<p>Configure the following information:</p> <ul style="list-style-type: none"> • Private key length • Common name • Email • Country • State/Province/Region • City • Organization • Department

7. Click **Apply**.



Downloading the Server Certificate

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


2. Click **Download Certificate**.
A dialog box appears.
3. Select **Certificate, Private Key**, or both.
4. Click **OK**.
QuTS hero downloads the selected files to your computer.

Managing a Root Certificate

1. Go to **Control Panel > System > Security > SSL Certificate & Private Key**.
2. Go to **Custom Root Certificate**.
3. Select one of the following actions:

Action	
Import a root certificate	<ol style="list-style-type: none"> a. Click Import. The Import Certificate window appears. b. Click Browse. The file upload window appears. c. Select a file. <div style="border-left: 2px solid red; padding-left: 10px; margin-left: 20px;">  <p>Important The root certificate file cannot be larger than 1 MB. The following file formats are supported: *.PFX, *.P12, *.PEM, *.crt, *.cer</p> </div> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Click . The Edit Root Certificate window appears. b. Edit the certificate description. c. Click Apply.
Delete a root certificate	<ol style="list-style-type: none"> 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: <code>user1</code> and password: <code>1resu</code> .
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 before their password expires**.
4. Click **Apply**.



Hardware

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

Configuring General Hardware Settings

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

Settings	User Action
Enable configuration reset switch	Select this option to enable the reset button. For details, see System Reset and Restore to Factory Default .

Settings	User Action
Enable disk standby mode	Select this option to allow the NAS drives to enter standby mode if there is no disk access within the specified period. Disk status LED remains on during standby mode.  Note Some QNAP NAS models that use NVMe solid-state drives do not support disk standby mode.
Enable light signal alert	Select this option to allow the status LED to flash when free space on the NAS is less than the set value.
Enable redundant power supply mode	Select this option to enable the redundant power supply.
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)	<p>Select from the two automatic fan speed adjustment options.</p> <ol style="list-style-type: none"> QuTS hero monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. QuTS hero adjusts the fan speed according to user-specified temperatures. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note Modes are only available for system fans.</p> <ul style="list-style-type: none"> • 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. </div>
Manually set fan speed	Move the slider to set the fan speed.

3. Click **Apply**.

Configuring Hardware Resource Settings

You can configure and allocate expansion card resources for different software QuTS hero applications in Hardware Resource Settings. You can also configure Thunderbolt expansion cards, 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	<p>QuTS hero applications share expansion card resources for transcoding.</p> <ul style="list-style-type: none"> • 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.

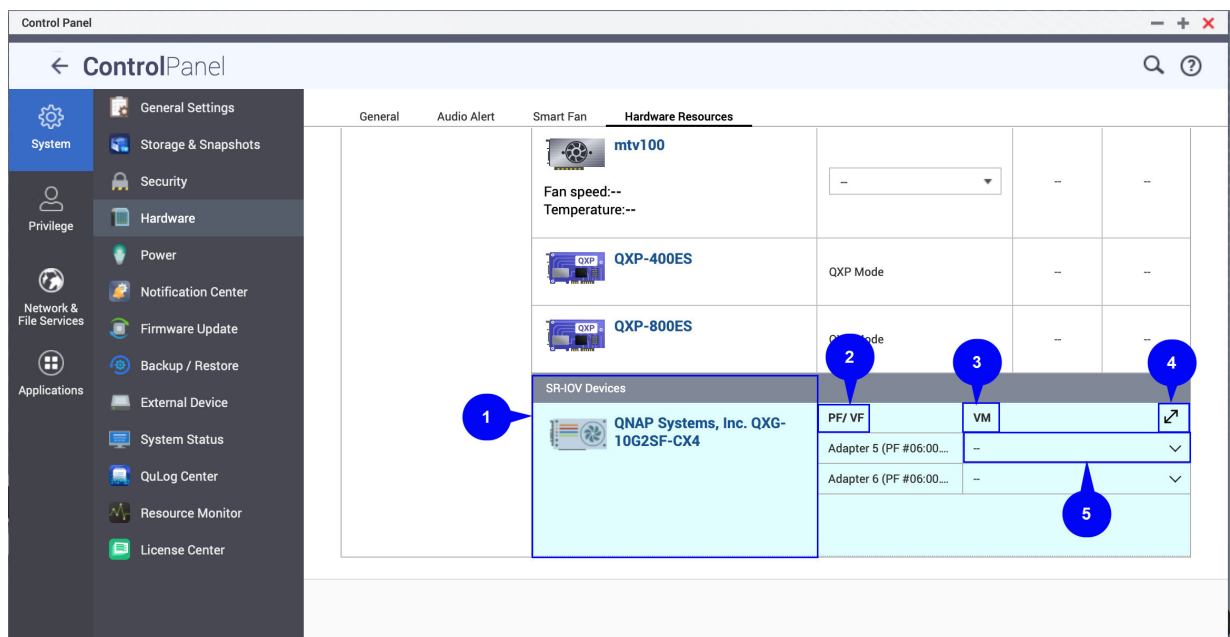
4. Click **Apply**.



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

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.

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)

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.

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

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


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

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	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note One schedule is shown by default.</p> <ol style="list-style-type: none"> a. Click Add. b. Select the following. <ul style="list-style-type: none"> • 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. </div> </div>

Task	User Action
Remove a scheduled action	<ol style="list-style-type: none"> a. Select one or mutiple 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. By default, QuTS hero will check for updates automatically every day. 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 .
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	<ul style="list-style-type: none"> • A computer <div style="margin-left: 20px;">  Important A computer is required for updating the firmware manually or through Qfinder Pro. </div> <ul style="list-style-type: none"> • Ethernet cables <div style="margin-left: 20px;">  Important QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection is reliable during firmware updates. </div>
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.

Settings	Requirements
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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> a. Click Path of firmware package file. b. Click Browse. c. Locate the downloaded firmware package file. d. Click OK.
Update firmware automatically	<ul style="list-style-type: none"> 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	<p>This resets the following settings to the default values without deleting the user data stored on the disks.</p> <ul style="list-style-type: none"> • 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. <p> 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".</p> <ul style="list-style-type: none"> • TCP/IP configuration: <ul style="list-style-type: none"> • 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. 	<ol style="list-style-type: none"> 1. Power on the NAS. 2. Press and hold the reset button for 3 seconds.

Option	Description	Steps
Advanced system reset	<p>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.</p> <p> Note To retrieve old data after an advanced system reset, re-create the previous folder structure on the NAS.</p>	<p>Perform an advanced system reset using one of the following methods.</p> <ul style="list-style-type: none"> • Using QuTS hero: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> a. Power on the NAS. b. Press and hold the reset button for 10 seconds.
Reinitialize the NAS	<p>This deletes all data on the disks and reinstalls QuTS hero.</p>	<ol style="list-style-type: none"> 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

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	<p>a. Connect the UPS to the NAS using a USB cable.</p> <p>b. Select USB connection.</p> <p>c. Choose one of the following options.</p> <ul style="list-style-type: none"> • 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 <p> 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.</p> <p>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.</p> <p> Note This option can only be selected when the UPS is connected to the NAS via USB.</p>
SNMP connection	<p>a. Connect the UPS to the same network as the NAS.</p> <p>b. Select SNMP connection.</p> <p>c. Specify the IP address of the UPS.</p> <p>d. Configure the SNMP community.</p> <p>e. Choose one of the following options.</p> <ul style="list-style-type: none"> • 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	<p>a. Connect the UPS to the same network as the NAS.</p> <p>b. Select Network UPS slave.</p> <p>c. Specify the IP address of the UPS server.</p> <p>d. Choose one of the following options.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p> Tip</p> <p>You can click More () and then select Settings to specify the time interval on the line charts.</p>
Storage Resource	<p>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.</p>
Processes	<p>This screen displays all ongoing background processes and provides information about each process, such as its current status, CPU usage, and memory usage.</p> <p> Tip</p> <p>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.</p>

4. Privilege Settings

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

Users

Default Administrator Account

The admin user account is the default administrator account. It can configure settings, create users, and install applications. You cannot delete this account. To prevent malicious actors from compromising your system due to easy passwords, QNAP strongly recommends changing the default admin password, creating another administrator account or logging in with an existing 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: <ul style="list-style-type: none"> • 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. <div style="margin-top: 10px;">  <p>Note Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.</p> </div>

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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
<p>Phone number (optional)</p>	<p>Specify a phone number that will receive SMS notifications from this device. For details, see SMS Notifications.</p> <p> Note Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.</p>
<p>Email (optional)</p>	<p>Specify an email address that will receive notifications from this device. For details, see Email Notifications.</p> <p> Note Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.</p>
<p>Send a notification mail to the newly created user (optional)</p>	<p>When selected, this device sends a message to the specified email address that contains the following information:</p> <ul style="list-style-type: none"> • Username and password • URLs for connecting to the NAS <p> Tip Users have the option to edit the notification message. To edit the notification message, follow these steps:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • Contain a space • Begin with the following characters: - # @ • Contain the following characters: @ " + = / \ : * ? < > ; [] % ` ' ` This prefix will be included before all usernames. Example: <code>test</code>
User Name Start No	Specify a start number with a maximum of 8 digits. Example: 1 <div style="margin-top: 10px;"> Note QuTS hero removes leading zeros in starting numbers. For example, 001 becomes 1. </div>
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.

- Click **Next**.
QuTS hero creates the user accounts and adds them to the displayed user list.
- Click **Finish**.

User Account Lists

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

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

Creating a TXT User File

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



Important

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



Note

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

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

- Save the list as a TXT file.

**Important**

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

Creating a CSV User File

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	<p>When selected, QuTS hero sends a message that contains the following information to the specified email address of the user.</p> <ul style="list-style-type: none"> • Username and password • URLs for connecting to the NAS <p> Important To send email notifications, ensure that you have configured an SMTP server. For details, see Configuring an Email Notification Server.</p>
Overwrite duplicate users	When selected, QuTS hero overwrites existing user accounts that have duplicates on the imported user account list.
User must change the password at first logon	When selected, the imported user must change the password when logging in for the first time. The password may contain a maximum of 64 ASCII characters.

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




Important

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

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

6. Click **Next**.

File Type	User Action
TXT or CSV	<p>The Import User Preview screen appears. Check the status of the user account list.</p> <p> Important The Status indicates whether any information is invalid. If any information is invalid, the user account list will not be imported successfully.</p>
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	<ol style="list-style-type: none"> 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
<p>Edit account profile</p>	<p>a. Under Action, click . The Edit Account Profile window appears.</p> <p>b. Edit the settings. The Edit Account Profile window provides the following settings not included in the Create a User window:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p>c. Optional: Disable the account.</p> <ol style="list-style-type: none"> 1. Select Disable this account. 2. Select when to disable the account. <ul style="list-style-type: none"> • Now: The account will be disabled after clicking OK. • Expiry date: The account will be disabled on the specified date. <p>d. Modify the quota for the user.</p> <p> Note This option is only available when quotas are enabled.</p> <ul style="list-style-type: none"> • 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. <p> Important Individual quotas may override group quotas.</p> <p>e. Click OK.</p>
<p>Edit user group</p>	<p>a. Under Action, click . The Edit User Group window appears.</p> <p>b. Select or deselect user groups.</p> <p>c. Click Apply.</p>

Task	User Action
Edit shared folder permission	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Under Action, click  . The Edit Application Privileges window appears. b. Select the applications that the user is allowed to access. c. Click Apply. <p> 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.</p>

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 maximum 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	<ul style="list-style-type: none"> a. Under Action, click  . The View Group Details window appears. b. Modify the description. c. Modify the quota. <p> Note</p> <ul style="list-style-type: none"> • 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. <p> Important Individual quotas may override group quotas. For details, see Quota Conflicts.</p> <ul style="list-style-type: none"> d. Click OK.

Task	User Action
Edit user group members	<ol style="list-style-type: none"> a. Under Action, click  . The Edit User Group window appears. b. Select or deselect users. c. Click Apply.
Edit shared folder permissions	<ol style="list-style-type: none"> 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. <p> Important Group-level permissions may override user-level permissions. For details, see Conflicts in Shared Folder Permissions.</p>

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	<p>This folder stores content from the Web Server utility, which you can manage in Control Panel > Applications > Web Server .</p> <p> Note You must enable Web Server automatically to create this default shared folder.</p>

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

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

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

7. Optional: Click **Enable snapshot schedule and snapshot retention**.




Note

By default, a snapshot is scheduled daily at 1:00 AM, and the snapshot retention policy is set to Smart Versioning. You can change these settings at any time. For details, see the following topics:

- [Configuring a Snapshot Schedule](#)
- [Configuring a Snapshot Retention Policy](#)


8. 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	<p>1 PB (1000 TB)</p> <p> 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.</p>

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




10. 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
<p>Save encryption key</p>	<p>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.</p> <p> Warning</p> <ul style="list-style-type: none"> • 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.


11. Click **Next**.

12. Optional: Configure any of the following storage settings.


Setting	Description
<p>Compression</p>	<p>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.</p> <p> Tip Compression does not impact read/write and processor performance on ZFS filesystems. Only disable this setting when necessary.</p>
<p>Deduplication</p>	<p>QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data.</p> <p> Important To enable deduplication your NAS must have at least 16 GB of memory.</p>
<p>SSD cache</p>	<p>QuTS hero adds data from this folder to the SSD cache to improve read performance.</p> <p> Important Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.</p>

Setting	Description
Fast clone	<p>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.</p> <p> Important</p> <ul style="list-style-type: none"> • 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.
Synchronous I/O	<p>Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes:</p> <ul style="list-style-type: none"> • 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	<p>Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application.</p> <p> Tip The default is 64K.</p>

- 13. 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	<p>Select a WORM type.</p> <ul style="list-style-type: none"> 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.
Lock delay	<p>When enabled, a file added to the folder can be modified or deleted within the lock delay time period. After this time has passed, the file automatically becomes locked and unmodifiable.</p> <p> Note</p> <ul style="list-style-type: none"> 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	<p>Limit how long WORM applies to each file and folder. Files and folders can be modified after the specified time period.</p>

14. Click **Next**.


15. 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](#).

16. Click **Next**.

17. 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 the kernel-mode SMB daemon is disabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.

Option	Description
Restrict the access of Recycle Bin to administrators only for now	<p>Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.</p> <p> Note This option is available only when Enable Network Recycle Bin is selected.</p>
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.
Set this folder as the Time Machine backup folder (macOS)	When enabled, the shared folder becomes the destination folder for Time Machine in macOS.

18. Click **Next**.

19. Review the summary information, and then click **Finish**.

QuTS hero creates the shared folder.

Editing Shared Folder Properties

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

Option	Description
Folder Name	<p>Specify a folder name that contains 1 to 64 characters and that does not:</p> <ul style="list-style-type: none"> • 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.

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 the kernel-mode SMB daemon is disabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	<p>Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.</p> <div data-bbox="592 712 651 772"></div> <p>Note This option is available only when Enable Network Recycle Bin is selected.</p>
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.
Set this folder as the Time Machine backup folder (macOS)	<p>When enabled, the shared folder becomes the destination folder for Time Machine in macOS.</p> <div data-bbox="592 1541 651 1601"></div> <p>Important</p> <ul style="list-style-type: none"> • 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	<p>Specify a folder name that contains 1 to 64 characters and that does not:</p> <ul style="list-style-type: none"> • End with a space • Contain consecutive spaces • End with "." • Begin with "_sn_" or "_sn_bk" • Contain the following characters: " + = / \ : * ? < > ; [] % ` ` ' " <p> 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.</p>
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.	<p>a. Click Next.</p> <p>b. Review the settings.</p>
	By User	Selecting this option allows you to configure access permissions to the ISO shared folder at the user level.	<p>a. Click Next.</p> <p>b. Configure the user account access rights for the ISO shared folder.</p> <p>c. Click Next.</p> <p>d. Review the settings.</p>
	By User Group	Selecting this option allows you to configure access permissions to the ISO shared folder at the user group level.	<p>a. Click Next.</p> <p>b. Configure the user group access rights for the ISO shared folder.</p> <p>c. Click Next.</p> <p>d. Review the settings.</p>

Type	Option	Description	User Action
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. <div style="display: flex; align-items: flex-start;">  <div> <p>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.</p> </div> </div>
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
<p>Users and groups permission</p>	<p>Edit user and user group permissions for shared folders that can be accessed through Windows, macOS, FTP, and File Station.</p>	<p>a. Optional: Select Individual permissions.</p> <p> 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.</p> <p>When selected, you can apply protocol-specific settings.</p> <p>1. Configuring for RW shared folders and RO subfolders:</p> <p>a. Select Read/Write permission for each user.</p> <p>b. Click  to delete the user group Everyone.</p> <p>c. Click Apply.</p> <p>d. Select a shared folder, and change permission style to Windows Special Permissions.</p> <p>e. Click  and select the following:</p> <ul style="list-style-type: none"> • 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 <p>f. Click OK.</p> <p>g. Optional: Add a user to the list of users with permissions for the shared folder.</p> <p>1. Click Add. The Add Users window appears.</p> <p>2. Select the following:</p> <ul style="list-style-type: none"> • Create files / write data • Create folder / append data • Write attributes

Permission Type	Description	User Action
<p>NFS host access</p>	<p>Edit NFS host access rights for shared folders.</p>	<p>a. Select Access right to enable NFS access rights.</p> <p> 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.</p> <p>b. Optional: Select any of the following options:</p> <ul style="list-style-type: none"> • sync Select a sync option for this setting. • secure <p>c. Under Host / IP / Network, enter an IP address or domain name.</p> <p>d. Optional: Add an NFS host. Under Allowed IP Address or Domain Name, click Add. QuTS hero adds an entry to the list.</p> <p>e. Optional: Delete an NFS host.</p> <ol style="list-style-type: none"> 1. Select an NFS host from the list. 2. Click Delete.
<p>Microsoft Networking host access</p>	<p>Specify which computers can access shared folders through Microsoft Networking.</p>	<p>a. Add a Microsoft Networking host.</p> <ol style="list-style-type: none"> 1. Click Add. QuTS hero adds an entry to the list. 2. Under Host / IP / Network, enter an IP address or domain name. <p>b. Optional: Delete a Microsoft Networking host.</p> <ol style="list-style-type: none"> 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 <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Enter the encryption password. b. Optional: Select Save encryption key. When enabled, QuTS hero automatically unlocks the shared folder after the NAS restarts. <p> Note This option is selected by default.</p>
Upload Encryption Key File	<ol style="list-style-type: none"> 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	<p>a. Go to Download.</p> <p>b. Enter the encryption password.</p> <p>c. Click OK. QuTS hero exports the encryption key file to your computer as a TXT.</p>
Save the encryption key	<p>a. Go to Save.</p> <p>b. Select Mount automatically on start up. When enabled, QuTS hero automatically unlocks the shared folder after the NAS restarts.</p> <p>c. Enter the encryption password.</p> <p>d. Click OK. QuTS hero saves the encryption key.</p>
Lock the shared folder	<p>a. Go to Lock.</p> <p>b. Optional: Select Forget the saved key.</p> <div data-bbox="531 882 587 943" style="float: left; margin-right: 10px;"></div> <p>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.</p> <p>c. Click OK. QuTS hero locks the folder.</p> <div data-bbox="531 1234 587 1294" style="float: left; margin-right: 10px;"></div> <p>Note</p> <ul style="list-style-type: none"> • Locked folders do not appear in File Station. A folder will only reappear after it is unlocked. • Users cannot edit the properties or permissions of a locked shared folder.

Shared Folder Access

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

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

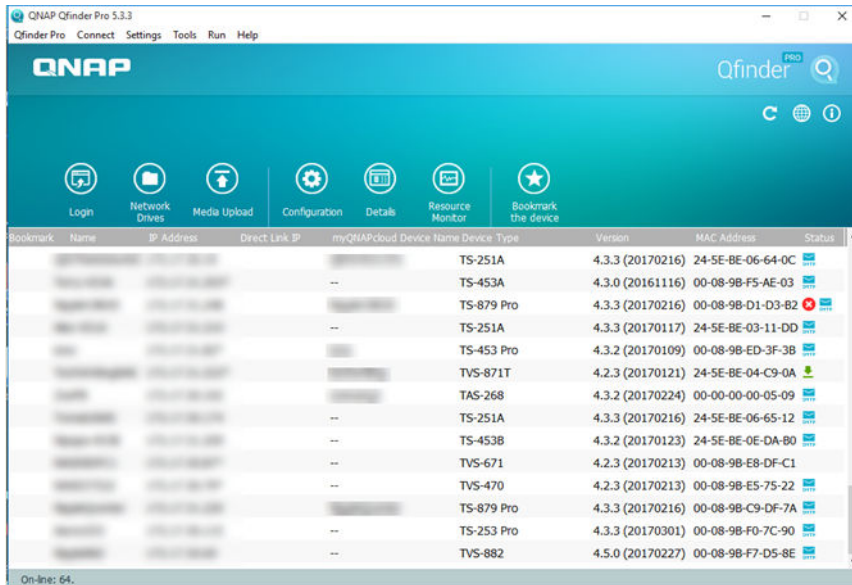
To download Qfinder Pro, go to <https://www.qnap.com/utilities>.

Mapping a Shared Folder on a Windows Computer

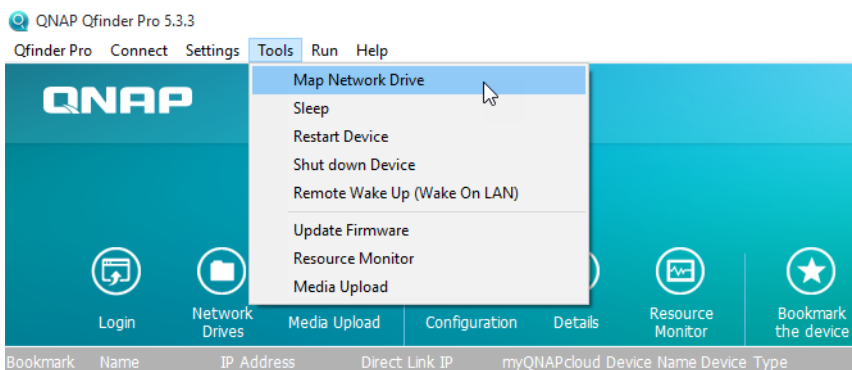
Before mapping a shared folder, ensure that you have Qfinder Pro installed on your Windows computer.

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

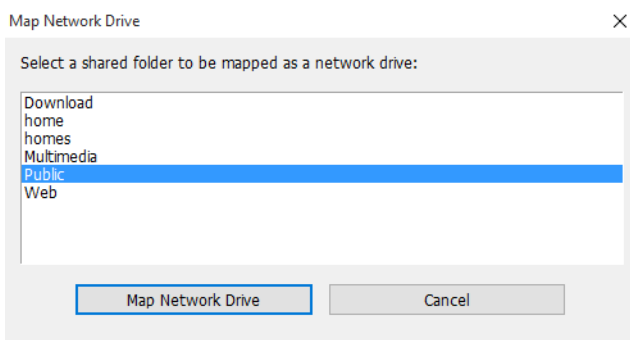
3. Open **Qfinder Pro**.
Qfinder Pro displays all QNAP NAS devices in your local area network.



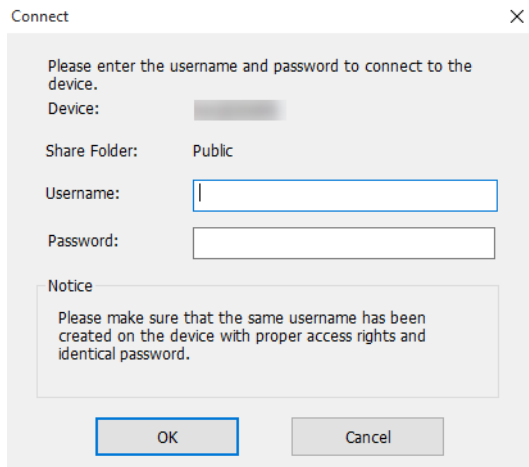
4. Select the NAS where the shared folder is located.
5. Click **Tools > Map Network Drive**.



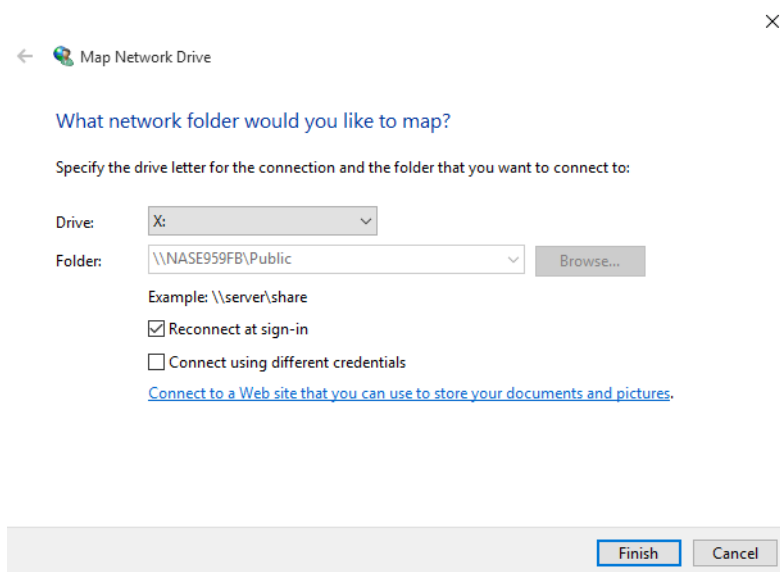
6. Select a shared folder.
7. Click **Map Network Drive**.



- 8. Specify your QuTS hero username and password.
- 9. Click **OK**.



- 10. Specify the following information.



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

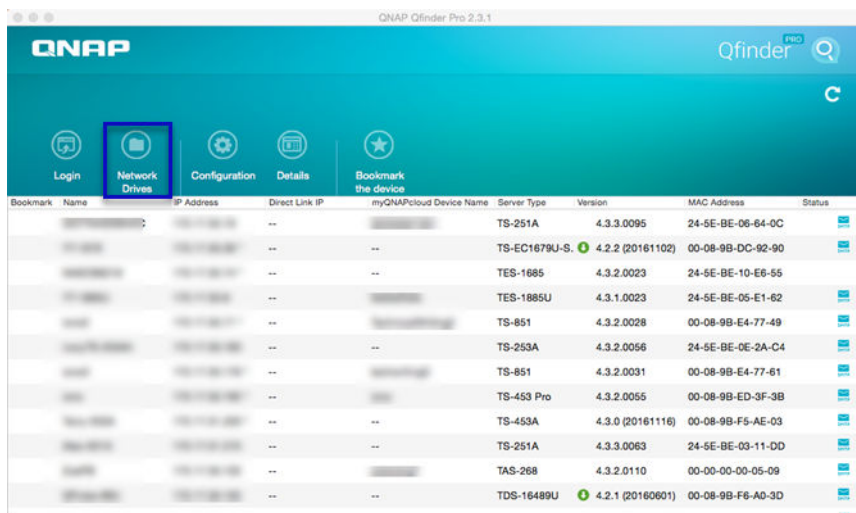
11. Click Finish.

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

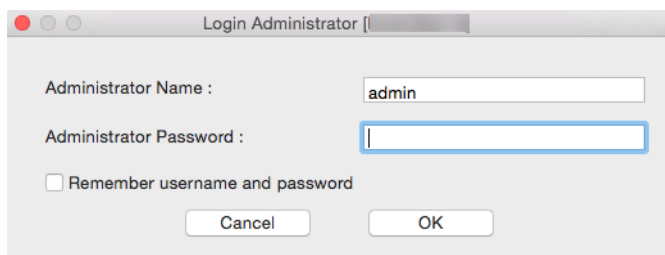
Mounting a Shared Folder on a Mac Computer

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

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

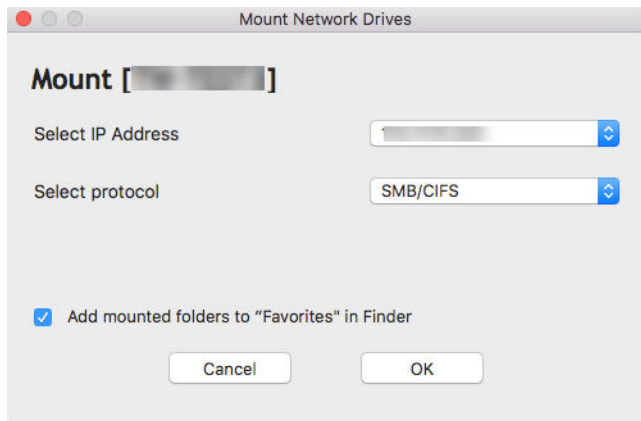


6. Specify your QuTS hero username and password.
7. Click **OK**.



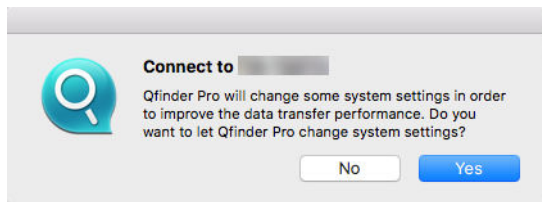
The **Mount Network Drives** window opens.

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

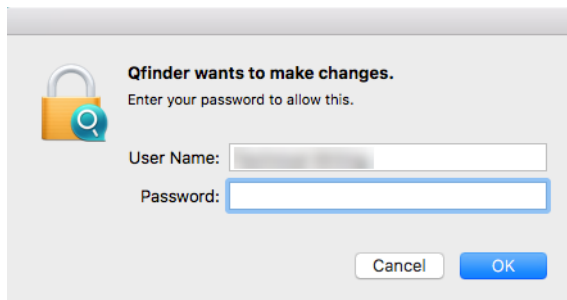


A confirmation message appears.

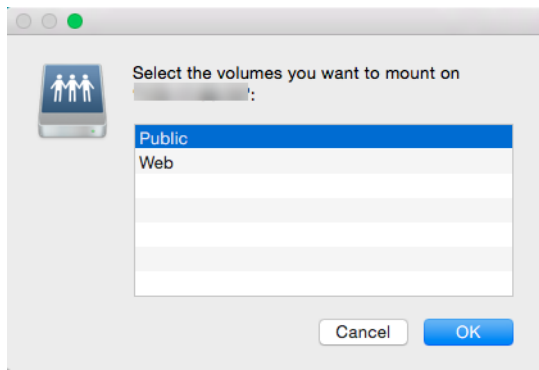
10. Click **Yes**.



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



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



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

Mounting a Shared Folder on a Linux Computer

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

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



Tip

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

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

3. Specify your NAS username and password.

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

Quota

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

QuTS hero provides three types of quota settings.

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

**Note**

Quotas are applied per shared folder and are not shared across shared folders.

**Important**

Individual quotas may override group quotas.
For details, see [Quota Conflicts](#).

**Tip**

You can export quota settings to a CSV file to use as a reference.
For details, see [Exporting Quota Settings](#).

Enabling Quotas

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

**Note**

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

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

Editing Quota Settings

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

**Tip**

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

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

**Note**

The quota must be between 100 MB and 128 TB.

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

**Important**

Individual quotas may override group quotas.
For details, see [Quota Conflicts](#).

6. Click **OK**.

Exporting Quota Settings

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

QuTS hero exports the quota settings as a CSV file.

Quota Conflicts

QuTS hero uses the following hierarchy to resolve quota conflicts.

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

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

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

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

**Note**

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

Domain Security

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

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

**Note**

QuTS hero supports AD running on Windows Server 2008 R2, 2012, 2012 R2, 2016, 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.

Option	Description
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. <ul style="list-style-type: none"> • ldap://: Use a standard LDAP connection. The default port is 389. • ldap:// (ldap + TLS): Use an encrypted connection with TLS. The default port is 389. Newer versions of LDAP servers normally use this port. • ldap:// (ldap + SSL): Use an encrypted connection with SSL. The default port is 686. Older versions of LDAP servers normally use this port.
	Base DN	Specify the LDAP domain. Example: <code>dc=mydomain,dc=local</code>
	Root DN	Specify the LDAP root user. Example: <code>cn=admin, dc=mydomain,dc=local</code>
	Password	Specify the root user password.
	Users Base DN	Specify the Organizational unit (OU) where users are stored. Example: <code>ou=people,dc=mydomain,dc=local</code>
	Group Base DN	Specify the OU where groups are stored. Example: <code>ou=group,dc=mydomain,dc=local</code>
	Current Samba ID	N/A
LDAP server of the remote NAS	IP address or NAS name	Specify the server IP address or the name of the NAS.
	LDAP domain	Specify the LDAP domain name.
	Password	Specify the NAS administrator password.
LDAP server of the local NAS	N/A	N/A
IBM Lotus Domino	This server type includes the same fields as Remote LDAP server , in addition to the following:	
	uidNumber	Specify the uid number. Select HASH .
	gidNumber	Specify the gid number. Select HASH .

- Click **Apply**.
The **LDAP authentication options** window appears.
- Select which users are allowed to access the NAS.



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

- Click **Finish**.

LDAP Authentication Options

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




Scenario	Options
Microsoft Networking is enabled before LDAP settings are applied.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> Under Action, click . The Edit Account Profile window appears. Edit the user quota. <p> Note User quotas must be enabled for this option to appear. For details, see Enabling Quotas.</p>
Edit shared folder permissions	<ol style="list-style-type: none"> Under Action, click . The Edit Shared Folder Permission window appears. Edit the user's permissions for each shared folder. For details, see Shared Folder Permissions.

Task	User Action
Edit application privileges	<p>a. Under Action, click  . The Edit Application Privileges window appears.</p> <p>b. Select the applications that the user is allowed to access.</p> <p> 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.</p>




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	<p>Under Action, click  . The View Group Details window appears. QuTS hero displays the group name and group users.</p>
Edit shared folder permissions	<p>a. Under Action, click  . The Edit Shared Folder Permission window appears.</p> <p>b. Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions.</p>



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: <ul style="list-style-type: none"> • Uppercase characters (A through Z) • Lowercase characters (a through z) • Base 10 digits (0 through 9) • Nonalphanumeric characters: ~!@#\$%^&* _-+=` \(){}[];'"<>.,?/
	Verify Password	Verify the administrator password.
<ul style="list-style-type: none"> • Additional Domain Controller • Read-Only Domain Controller 	Domain	Specify the domain.
	Domain DNS IP	Specify the domain DNS IP.
<ul style="list-style-type: none"> • Read-Only Domain Controller 	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: <ul style="list-style-type: none"> • Begin with a space • Begin with the following characters: - # @ • Contain the following characters: " + = / \ : * ? < > ; [] % ` ' `

Field	Description
Password	Specify a password between 8 and 127 characters that contains at least three of the following: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <div style="border-left: 1px solid #0070C0; padding-left: 10px; margin-left: 10px;">  Note QuTS hero removes leading zeros in starting numbers. For example, 001 becomes 1. </div>
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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Under Action, click  . The Change Password window appears. b. Specify a password that meets the requirements. c. Verify the password. d. Click Change.

Task	User Action
Edit user properties	<p>a. Under Action, click . The Edit User Properties window appears.</p> <p>b. Edit the user properties. For details, see Creating a Domain User.</p> <p>c. Click Finish.</p>
Edit user group membership	<p>a. Under Action, click . The Edit User Groups wizard appears.</p> <p>b. Select or deselect user groups. For details, see Domain User Groups.</p> <p>c. Click Next.</p> <p>d. Review the summary, and then click Finish.</p>
Edit user profile	<p>a. Under Action, click . The Edit User Profile window appears.</p> <p>b. Specify the following:</p> <ul style="list-style-type: none"> • 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. <p>• Click Finish.</p>



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: <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
Type	Select the type of record.

6. Modify the values.

Task	User Action
Add a value	<ol style="list-style-type: none"> a. Specify a value. b. Click . The value is added to the list.
Move a value up	<ol style="list-style-type: none"> a. Select a value from the list. b. Click . The value moves up in the list.

Task	User Action
Move a value down	<p>a. Select a value from the list.</p> <p>b. Click . The value moves down in the list.</p>
Remove a value	<p>a. Select a value from the list.</p> <p>b. Click . The value is removed from the list.</p>

7. Click **Apply**.

Adding Domains

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



Note

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

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

Adding Records

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



Note

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.

3. Select a domain or record.

4. Click **Action > Add Record** .
The **Add New Record** window appears.
5. Specify the following information.

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

6. Click **Create**.

Deleting Domains or Records

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



Note

This is the account created when enabling the domain controller.

- a. Specify the following information.

Field	Description
Account	Enter <code>administrator</code> .
Password	Enter the password specified when the account was created.

- b. Click **Login**.
3. Select a domain or record to delete.
4. Click **Action > Delete** .
A warning message appears.
5. Click **Yes**.

Back Up/Restore

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

Backing Up Domain Controllers

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

Option	Description
Backup frequency	Select how often the Active Directory Domain Controller (ADDC) database is backed up.
Start Time	Select when the backup will begin.
Destination folder	Select the NAS folder where the backup will be stored.
Backup Options	Select one of the following: <ul style="list-style-type: none"> • Overwrite existing backup file (dc_backup.exp) • Create a new file for each backup and append the date to the filename (dc_backupyyyy_mm_dd_exp)

4. Click **Apply**.

Restoring Domain Controllers



Important

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



Warning

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

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

5. Services


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: Update the antivirus with one of the following methods.

Option	User Action
Update now	Click Update now . The system immediately updates the antivirus.
Update automatically	<ol style="list-style-type: none"> a. Select Check and update automatically. b. Specify the frequency. The system automatically checks for antivirus updates on the specified date.
Update manually	<ol style="list-style-type: none"> a. Click Browse. An upload window appears. b. Select a virus database file (.cvd) to upload. <div style="border-left: 2px solid #ffc107; padding-left: 10px; margin: 10px 0;">  Tip You can download the latest ClamAV virus database file from http://www.clamav.net/. </div> <ol style="list-style-type: none"> c. Click Import.

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	<p>a. Click Specific folders.</p> <p>b. Select a shared folder from the drop-down menu.</p> <p>c. Click Add.</p> <p> Tip To remove a shared folder, click .</p>


6. Click **Next**.
The **Schedule** screen appears.
7. Select a scan frequency option and configure the settings if required.
8. Click **Next**.
The **File Filter** screen appears.
9. Select one of the following file filter options:

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

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

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





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

Option	Description
Only report the virus	QuTS hero only reports detected viruses and does not take any further action. The detections will appear in Reports .
Move infected files to quarantine	QuTS hero quarantines the infected files. You cannot access these files from shared folders. You can review the virus scan report in Reports and delete or restore infected files in Quarantine .
Delete infected files automatically	<p>QuTS hero deletes the infected files.</p> <div style="display: flex; align-items: center;">  <div> <p>Important</p> <p>These files are permanently deleted.</p> </div> </div>

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

Managing Scan Jobs

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

Option	User Action
Run now	<p>Select .</p> <p>QuTS hero starts the scan job.</p>
Edit	<ol style="list-style-type: none"> a. Select . <p>The Details window opens.</p> b. Modify the settings. c. Click OK. <p>QuTS hero modifies the scan job's settings.</p>
View last run log	<ol style="list-style-type: none"> a. Select . <p>The Last run log window opens.</p> b. Optional: Click the text box to modify the run log. c. Click Close.
Delete	<ol style="list-style-type: none"> a. Select . <p>A confirmation message appears.</p> b. Click Yes. <p>QuTS hero deletes the scan job.</p>

Managing Reported Scan Jobs




1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > Antivirus > Reports** .
3. Optional: Specify the log retention period.
 - a. Go to **Number of days to keep the logs**.

- b. Enter the number of days.



Tip
Enter a number between 1 to 999.

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


Option	User Action
Download	Select  . QuTS hero downloads the scan job as a text document to your computer.  Tip To download all job logs, click Download All Logs .
Delete	<ul style="list-style-type: none"> a. Select . A confirmation message appears. b. Click Yes. QuTS hero deletes the scan job.



Managing Quarantined Files



Warning
You cannot recover deleted quarantined files.

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

Option	User Action
Delete	Click  . QuTS hero permanently deletes the selected file.
Delete Selected Files	<ul style="list-style-type: none"> a. Select files. b. Click Delete Selected Files. Only selected files in the list are permanently deleted.
Delete All Files	Click Delete All Files . All files in the list are permanently deleted.

Option	User Action
Restore	Click  . QuTS hero restores the file to its shared folder.
Restore Selected Files	<p>a. Select files.</p> <p>b. Click Restore Selected Files. Only selected files in the list are restored to their shared folders.</p>
Exclude List	Click  . QuTS hero restores the file to its shared folder and adds the file to the exclude list.

Servers



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




Web Server

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

Enabling the Web Server

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > Web Server > Web Server** .
3. Select **Enable Web Server**.
4. Optional: Configure the following settings.

Setting	User Action
Port number	Specify a port number.  Note The default port is 80.
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.

Setting	User Action
<p>Enable secure connection (HTTPS)</p>	<p>Select this option to allow HTTPS connections.</p> <ol style="list-style-type: none"> Select Enable secure connection (HTTPS). Select a TLS version. The default TLS version is 1.2. <p> Warning Selecting the latest TLS version may decrease compatibility for other clients in your system.</p> <ol style="list-style-type: none"> Enable strong cipher suites. Specify a port number. <p> Note The default port is 8081.</p> <ol style="list-style-type: none"> Optional: Select Force secure connection (HTTPS) only to require all users to connect to the NAS using only HTTPS.
<p>Maximum number of clients</p>	<p>Enter a maximum client number.</p> <p> Note A client number is the number of users that are allowed to connect to the server.</p>
<p>Do not allow QTS embedding in IFrames</p>	<ol style="list-style-type: none"> Select this option to prevent websites from embedding QuTS hero using IFrames. Click Allowed Websites to allow a specific website to embed QuTS hero in IFrames. The Allowed Websites window appears. Optional: Click Add to add a website to the list. The Add Host Name window appears. Specify a host name. Click Add. The host name is added to the allowed websites list. Optional: Select a website, and then click Delete to delete a website from the list. Click Apply.
<p>Enable X-Content-Type-Options HTTP header</p>	<p>Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities.</p>
<p>Enable Content Security Policy HTTP header</p>	<p>Select this option to protect your device from attacks that exploit Cross Site Scripting (XSS) and data injection vulnerabilities.</p>

5. Click **Apply**.

**Tip**

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

QuTS hero enables the web server.

Modifying the php.ini Maintenance File

The php.ini file is the default PHP configuration file. To optimize your website performance, you can modify and configure the default settings in the php.ini file, such as execution time, memory limit, and maximum file upload size.

**Important**

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. Below **php.ini Maintenance**, select one of the following options.

Option	User Action
Upload	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Click Edit. The Edit php.ini window opens. b. Edit the php.ini file. c. Click Apply. QuTS hero saves the changes.
Restore	<ol style="list-style-type: none"> a. Click Restore. A confirmation message appears. b. Click OK. QuTS hero restores the default php.ini file.

Enabling and Creating a Virtual Host

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

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > Web Server > Virtual Host** .
3. Select **Enable Virtual Host**.
4. Click **Apply**.
You can now create a virtual host.

5. Click **Create a Virtual Host**.
The **Advanced Options** window opens.
6. Enter a host name.
7. Select a root directory.
8. Select a protocol.
9. Enter a port number.
10. Click **Apply**.
The virtual host appears in the Host Name list.

Enabling the LDAP Server

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

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > LDAP Server**.
3. Select **Enable LDAP Server**.
4. Enter a domain name.
5. Specify a password.
6. Verify the password.
7. Select a TLS version.
8. Optional: Click **Initialize**.



Warning

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

9. Click **Apply**.

MariaDB Server

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

MariaDB Server Requirements

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

Configuring the MariaDB Database



Important

- If the SQL server was enabled in QTS 4.5.4 (or earlier) before you updated to QTS 5.0.0 (or later), after the update the system will have automatically downloaded and installed the MariaDB 5 app and migrated the SQL server data to MariaDB.
- You can install either the MariaDB 5 or MariaDB 10 app. If you install both app versions on your NAS, MariaDB 5 will be set as the default database server.

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

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

Creating a MariaDB Database



Warning

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

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



Note

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

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



Important

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

- If the system detects a weak password, the MariaDB server will be automatically disabled until a stronger password is configured.

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



Tip

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

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



Note

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

10. Click **Finish**.
QuTS hero enables the MariaDB server.

Restoring a MariaDB Database

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



Note

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

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



Note

This option is enabled by default.

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



Note

The default port is 3307.

7. Click **Apply**.

QuTS hero restores the MariaDB database. The **Finish** screen appears.



Note

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

8. Click **Finish**.
QuTS hero enables the MariaDB server.

Migrating a MariaDB 5 Database to MariaDB 10

This feature is only available in the MariaDB 10 app.

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



Note

For details, see [Installing an App from App Center](#).

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



Note

The MariaDB setup wizard only appears during app initialization. To configure more advanced database features and settings, edit the php.ini maintenance file. For details, see [Modifying the php.ini Maintenance File](#).

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



Note

This option is enabled by default.

- b. Specify the TCP/IP networking port.



Note

The default port is 3307.

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



Note

The data migration may take a few minutes to complete.

9. Click **Finish**.
QuTS hero enables the MariaDB server.



Enabling or Disabling the MariaDB Server



Important

If the SQL server was enabled in QTS 4.5.4 (or earlier) before you updated to QTS 5.0.0 (or later), after the update the system will have automatically downloaded and installed the MariaDB 5 app and migrated the SQL server data to MariaDB.


1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > MariaDB** .
The MariaDB app opens.
3. Perform one of the following operations:

Options	User Actions
Enable the MariaDB server	Click  .
Disable the MariaDB server	Click  .

Managing the MariaDB Account and Database

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > MariaDB** .
The MariaDB app opens.
3. Click **Account and Database**.
4. Perform any of the following:

Option	User Action
Reset the root password	<div data-bbox="593 257 651 324"></div> <p>Warning Resetting the root password will restart the MariaDB database.</p> <div data-bbox="593 392 651 459"></div> <p>Important To protect your NAS, the system will automatically detect weak MariaDB server root passwords and require you to change the password. Follow the on-screen instructions to change the root password.</p> <p>a. Click Reset. The Reset Root Password screen appears.</p> <p>b. Specify a new password.</p> <div data-bbox="593 739 651 806"></div> <p>Note</p> <ul style="list-style-type: none"> • The password must contain 8 to 64 bytes of UTF-8 characters. • The password cannot be "admin" or blank. <p>c. Confirm the password.</p> <p>d. Click Next. A confirmation message appears.</p> <p>e. Click Yes. The root password is changed.</p>
Reset user passwords	<p>a. Click Reset. The Reset User Passwords screen appears.</p> <p>b. Enter the root password.</p> <p>c. Click Next.</p> <p>d. Select a user account.</p> <p>e. Specify a new password.</p> <div data-bbox="593 1500 651 1568"></div> <p>Note</p> <ul style="list-style-type: none"> • The password must contain 8 to 64 bytes of UTF-8 characters. • The password cannot be "admin" or blank. <p>f. Confirm the password.</p> <p>g. Click Apply.</p>

Option	User Action
Reinitialize the database	 <p>Warning Reinitializing the database will delete all data in the database.</p> <ol style="list-style-type: none"> a. Click Reinitialize. A confirmation message appears. b. Click Yes. The MariaDB Setup Wizard screen appears.

Modifying the TCP/IP Network Settings

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



Note

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

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

Syslog Server

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

Enabling the Syslog Server

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > Syslog Server > Server Settings** .
3. Select **Enable Syslog Server**.
4. Select at least one of the following options.

Option	User Action
Enable TCP	<ol style="list-style-type: none"> a. Select Enable TCP. b. Enter a TCP port.
Enable UDP	<ol style="list-style-type: none"> a. Select Enable UDP. b. Enter a UDP port.

5. Optional: Configure the log settings.

- a. Specify the maximum log size.

**Tip**

The log size range is 1 to 100.

- b. Select the log destination folder.

- c. Enter the log file name.

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.

For details, see [Creating an Event Notification Rule](#).

Adding a Syslog Server Filter

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

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > Syslog Server > Filter Settings**.
3. Click **Add a Filter**.
The **Add a Filter** window opens.
4. Configure the filter.
 - a. Select the filter type.
 - **Facility**
 - **Severity**
 - **Hostname**
 - **Application**
 - **Message**
 - **IP**

- b. Select a filter option.
 - **greater than or equal to**
 - **less than or equal to**
 - **equals**
 - **starts with**
 - **contains**
 - **not equals**
 - **does not start with**
 - **does not contain**
- c. Enter the filter condition.
- d. Click **Add**.






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

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

Managing Syslog Filters

- 1. Log on to QuTS hero as administrator.
- 2. Go to **Control Panel > Applications > Syslog Server > Filter Settings** .
- 3. Locate the filter you want to modify.
- 4. Perform one of the following options.

Option	User Action
Enable	Click  . QuTS hero enables the filter.
Disable	Click  . QuTS hero disables the filter.
Edit	<ul style="list-style-type: none"> a. Click . The Filter window opens. b. Modify the filter. c. Click Apply. QuTS hero saves the filter information.

Option	User Action
Delete	<ol style="list-style-type: none"> a. Select one or more filters. b. Click Delete. A confirmation message appears. c. Click Yes. QuTS hero deletes the selected filters.

**Tip**

To view syslog messages, 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 the RADIUS Server

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

**Note**

This option allows local NAS users to access network services using the login credentials for RADIUS clients.

5. Click **Apply**.




Creating a RADIUS Client

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

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

Managing RADIUS Clients

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Applications > RADIUS Server > RADIUS Clients** .
3. Locate the client you want to modify.
4. Perform one of the following options.

Option	User Action
Enable	Click  . QuTS hero enables the client.
Disable	Click  . QuTS hero disables the client.
Edit	<ol style="list-style-type: none"> a. Click . The Edit Client window opens. b. Configure the client information. c. Click Apply. QuTS hero saves the client information.
Delete	<ol style="list-style-type: none"> a. Select one or more clients. b. Click Delete. A confirmation message appears. c. Click Yes. QuTS hero deletes the selected clients.

Creating a RADIUS User




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

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

Managing RADIUS Users

1. Log on to QuTS hero as administrator.

2. Go to **Control Panel > Applications > RADIUS Server > RADIUS Users** .
3. Select one of the following options.

Option	User Action
Enable	Click  . QuTS hero enables the user.
Disable	Click  . QuTS hero disables the user.
Change Password	<ol style="list-style-type: none"> a. Click . The Edit User window opens. b. Modify the settings. c. Click Apply. QuTS hero saves the new password.
Delete	<ol style="list-style-type: none"> a. Select one or more users. b. Click Delete. A confirmation message appears. c. Click Yes. QuTS hero deletes the selected users.

Enabling the TFTP Server

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

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



Note

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

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



Note

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

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

Option	Description
Anywhere	Allows TFTP access from any IP address.
Certain IP range only	Allows TFTP access from IP addresses in the specified IP range only. Enter the start and end IP addresses of the IP range.

- Click **Apply**.
QuTS hero enables the TFTP server.

Enabling the NTP Server

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

- Log on to QuTS hero as administrator.
- Go to **Control Panel > Applications > NTP Server** .
- Select **Enable NTP Server (NTP server is Ready)**.
- 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.

- Click **Apply**.
QuTS hero enables the NTP server.

6. 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	<ul style="list-style-type: none"> • 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.

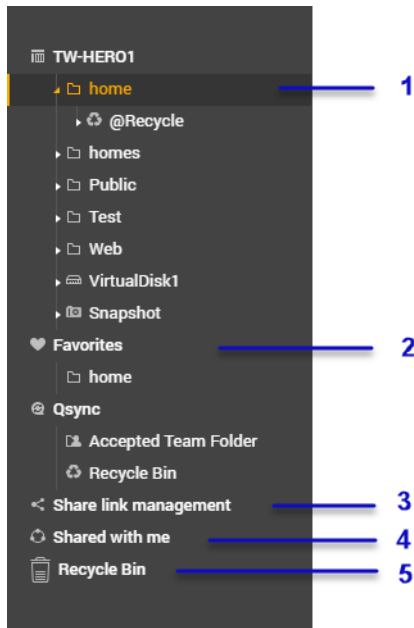
Supported File Formats

Category	File Extension
Image	<ul style="list-style-type: none"> • BMP • JPG • JPE • PNG • TGA • GIF • HEIC • HEIF
Music	<ul style="list-style-type: none"> • MP3 • FLAC • OGG • WAV • AIF • AIFF

Category	File Extension
Video	<ul style="list-style-type: none"> • 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. <div style="display: flex; align-items: center;"> <div> <p>Note Users in the administrator group can see links shared by all NAS users.</p> </div> </div>
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.

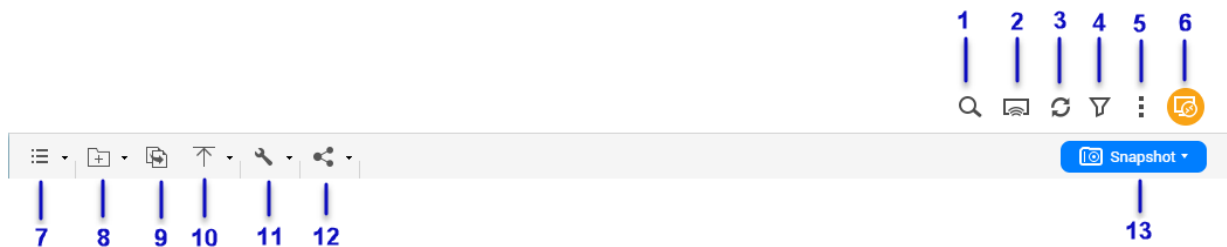
Folder	Description
Snapshot	Displays the saved snapshots.


Folder	Description
Local folders	<p>Displays the local folders on a Windows computer.</p> <p> Important To view local folders from File Station, you must first install Java Runtime Environment.</p>
Qsync	Displays files, folders, and team folders from Qsync.
VJBOD Cloud shared folder	<p>Displays files and folders from a shared folder created on a VJBOD Cloud Volume.</p> <p> 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.</p>




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	<p>Search files and folders by their name or type.</p> <p> Tip You can select Advanced Search to specify more criteria.</p>
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	<ul style="list-style-type: none"> • Always ask me • Rename duplicate files • Skip duplicate files • Overwrite duplicate files
When copying or moving files	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.  Note To enable this feature, you must install and start Multimedia Console from the App Center.
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	<ul style="list-style-type: none"> • Always ask me • View in Google Docs • Open with Chrome Extension • Open with web browser
For .docx, .pptx, .xlsx files	<ul style="list-style-type: none"> • Always ask me • Edit with Office Online • View in Google Docs • Open with Chrome Extension • Open with web browser

- 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.

- Click **Apply**.
- 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.

- Click  on the top-right corner.
- Select **Settings**.
The **Options** window appears.
- Select **Third-party Service**.
- 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>

- Paste your CloudConvert API key.
- Click **Apply**.

File Operations


File Station enables you to perform the following tasks.

Operation	Task
Store	<ul style="list-style-type: none"> • Uploading a File
Access	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Playing an Audio File • Playing a Video File • Opening a 360-degree Image or Video File • Streaming to a Network Media Player
Transcode	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Click  and then select File. The File Upload window opens. b. Select the file and then click Open.
Using drag and drop	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<p>a. Select the file.</p> <p>b. Click .</p> <p>c. Select Open.</p>
Using the context menu	Right-click and then select Open .
Open the file directly	<p>Double-click the file.</p> <p> Note</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<p>a. Select the file.</p> <p>b. Click .</p> <p>c. Select Open with Chrome Extension.</p>
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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Open with Text Editor.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Properties.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Properties.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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	<p>a. Right-click the file and then select Copy to/Move to and Move to.</p> <p>b. Select the destination folder.</p> <p>c. Click OK.</p>
	<p>a. Right-click the file and then select Cut.</p> <p>b. Select the destination folder.</p> <p>c. Right-click inside the folder and then select Paste.</p>
Using keyboard shortcuts	<p>a. Select the file.</p> <p>b. Press CTRL + X or Command-X.</p> <p>c. Go to the destination folder.</p> <p>d. Press CTRL + V or Command-V.</p>
Using drag and drop	<p>a. Select the file.</p> <p>b. Drag and drop to the destination folder.</p> <p>c. Step result: A context menu appears.</p> <p>d. Select one of the following actions.</p> <ul style="list-style-type: none"> • 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	<p>a. Select the file.</p> <p>b. Click .</p> <p>c. Select Rename.</p>
Using the context menu	<p>a. Right-click the file.</p> <p>b. Select Rename.</p>
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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Delete.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Recover.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Mount ISO.
Using the context menu	<ol style="list-style-type: none"> 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	<p>a. Select the file or folder.</p> <p>b. Click .</p> <p>c. Select Compress(Zip).</p>
Using the context menu	<p>a. Right-click the file or folder.</p> <p>b. Select Compress(Zip).</p>


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. <ul style="list-style-type: none"> • Normal - Standard compression • Maximum compression - Prioritizes compression quality • Fast compression - Prioritizes compression speed
Archive format	Select the format of file compression. <ul style="list-style-type: none"> • zip • 7z
Update mode	Specify how the files should be updated. <ul style="list-style-type: none"> • 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	<p>a. Select the file or folder.</p> <p>b. Click Share.</p> <p>c. Select Via Email.</p>
Using the context menu	<p>a. Right-click the file or folder.</p> <p>b. Select Share.</p> <p>c. Select Via Email.</p>







The **Share** window appears.

4. Configure the following settings.

Field	User Action
Send from	<p>Select the email delivery method.</p> <ul style="list-style-type: none"> • Use NAS to mail the links. • Use local computer to mail the links.
Sender	Select an email account.
To	<p>Specify the email address of the recipient.</p> <p> Tip You can select a recipient from your contact list if Qcontactz is installed on the NAS.</p>
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	<p>Enter a name for the link or use the current name of the file or folder.</p> <p> Note A link name cannot contain the following characters: / \ : ? < > * "</p>

Field	User Action
Domain name/IP	<p>Select the domain name or IP address.</p> <p> Tip The following domains and IP addresses are supported:</p> <ul style="list-style-type: none"> • 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. <p> Note The recipients get direct read access.</p>
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	<p>Allow users to transcode videos on the fly.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>Allow users to upload files to this folder.</p> <p> Note This setting only appears when sharing folders.</p>
Expire in	<p>Specify the expiration date.</p> <p> Note You cannot access the shared file or folder after the expiration date.</p>
Password	<p>Require a password to access the link.</p> <p> Tip To include the password in the email, select Show the password in the email.</p>

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	<ol style="list-style-type: none"> a. Select the file or folder. b. Click Share. c. Select To Social Network.
Using the context menu	<ol style="list-style-type: none"> 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	<p>Type a name for the link or use the current file or folder name.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Note A link name cannot contain the following characters: / \ : ? < > * "</p> </div> </div>

Field	User Action
Domain name/IP	<p>Select the domain name or IP address.</p> <p> Tip The following domains and IP are supported:</p> <ul style="list-style-type: none"> • 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. <p> Note The recipients get direct read access.</p>
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	<p>Allow users to transcode videos on the fly.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>Allow users to upload files to this folder</p> <p> Note This setting only appears when sharing folders.</p>
Expire in	<p>Specify the expiration date.</p> <p> Note You cannot access the shared file or folder after the expiration date.</p>
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	<ol style="list-style-type: none"> a. Select the file or folder. b. Click Share. c. Select Create share link only.
Using the context menu	<ol style="list-style-type: none"> 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	<p>Type a name for the link or use the current file or folder name.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note A link name cannot contain the following characters: / \ : ? < > * " </div>
Domain name/IP	<p>Select the domain name or IP address.</p> <div style="border-left: 2px solid #FFC000; padding-left: 10px; margin-top: 10px;">  Tip The following domains and IP are supported: <ul style="list-style-type: none"> • 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. </div> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note The recipients get direct read access. </div>
Show SSL in URL	Use an HTTPS URL.
On-the-fly transcoding	<p>Allow users to transcode videos on the fly.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note <ul style="list-style-type: none"> • 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). </div>

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	<ol style="list-style-type: none"> a. Select the file or folder. b. Click Share. c. Select To NAS user.
Using the context menu	<ol style="list-style-type: none"> 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	<p>Type a name for the link or use the current file or folder name.</p> <p> Note A link name cannot contain the following characters: / \ : ? < > * "</p>
Domain name/IP	<p>Select the domain name or IP address.</p> <p> Tip The following domains and IP are supported:</p> <ul style="list-style-type: none"> • 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. <p> Note The recipients get direct read access.</p>
Show SSL in URL	<p>Use an HTTPS URL.</p>
On-the-fly transcoding	<p>Allow users to transcode videos on the fly.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>Allow users to upload files to this folder</p> <p> Note This setting only appears when sharing folders.</p>
Expire in	<p>Specify the expiration date.</p> <p> Note You cannot access the shared file or folder after the expiration date.</p>

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

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

Playing an Audio File

- Open File Station.
- Locate the file.
- Perform one of the following methods.


Method	Steps
Using the toolbar	<ol style="list-style-type: none"> Select the file. Click . Select Play.
Using the context menu	<ol style="list-style-type: none"> Right-click the file. 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.

- Open File Station.
- Locate the file.
- Perform one of the following methods.

Method	Steps
Using the toolbar	<ol style="list-style-type: none"> Select the file. Click . Select Play. Select a resolution.
Using the context menu	<ol style="list-style-type: none"> Right-click the file.

	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Click Play with CAYIN MediaSign Player.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Play.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<p>a. Select the file.</p> <p>b. Click .</p> <p>c. Select Add to Transcode.</p>
Using the context menu	<p>a. Right-click the file.</p> <p>b. Select Add to Transcode.</p>

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	<p>a. Select the file.</p> <p>b. Click .</p> <p>c. Select Cancel/Delete Transcoding.</p>
Using the context menu	<p>a. Right-click the file.</p> <p>b. Select Cancel/Delete Transcoding.</p>

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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Transcode Information.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Extract.
Using the context menu	<ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> • Uploading a Folder • Uploading a Folder Using Drag and Drop
Access	<ul style="list-style-type: none"> • Viewing Folder Properties • Viewing Storage Information • Modifying Folder Permissions • Viewing Qsync Folders • Managing Share Links • Viewing Files and Folders Shared with Me
Organize	<ul style="list-style-type: none"> • Creating a Folder • Copying a Folder • Creating a Desktop Shortcut • Adding a Folder to Favorites • Removing a Folder from Favorites • Compressing a Folder
Share	<ul style="list-style-type: none"> • Creating a Shared Folder • Sharing Space with a New User
Transcoding	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Properties.

Method	Steps
Using the context menu	<ol style="list-style-type: none"> a. Right-click the folder. b. Select Properties.
Use the left panel	<ol style="list-style-type: none"> 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	<p>Keeps track of access to the folder.</p> <div style="display: flex; align-items: center;">  <div> <p>Tip To enable this feature, select Track file and folder access in File Station > Options .</p> </div> </div>
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	<ol style="list-style-type: none"> a. Select the folder.

	<ol style="list-style-type: none"> b. Click . c. Select Storage Info.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Properties.
Using the context menu	<ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Click . b. Select Folder. The Create folder window opens. c. Specify the folder name. d. Click OK.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Create Shortcut to Desktop.
Using the context menu	<ol style="list-style-type: none"> a. Right-click the folder. b. Select Create Shortcut to Desktop.
Drag and Drop	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Add to Favorites.
Using the context menu	<ol style="list-style-type: none"> a. Right-click the folder. b. Select Add to Favorites.
Use the Favorites button	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Remove from Favorites.
Using the context menu	<ol style="list-style-type: none"> a. Right-click the folder. b. Select Remove from Favorites.
Use the Favorites button	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Compress(Zip).
Using the context menu	<ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> • Normal - Standard compression • Maximum compression - Prioritizes compression quality • Fast compression - Prioritizes compression speed
Archive format	Select the format of file compression. <ul style="list-style-type: none"> • zip • 7z
Update mode	Specify how the files should be updated. <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Delete.
Using the context menu	<ol style="list-style-type: none"> 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** window opens.
4. Specify a shared folder name.
 - The name can be in any Unicode language.
 - The maximum length is 64 bytes. In English, this equals 64 characters.
 - The following special characters are not allowed: @ " + = / \ : | * ? < > ; [] % , ` ' non-breaking space
 - The last character cannot be a period (.) or space.
 - The name cannot begin with a space or "_sn_".
5. Optional: Specify a description.
The information is for your reference and is not used by QuTS hero.
6. Select a storage pool.
The shared folder is created using storage space from this pool.
7. Select a method of space allocation.

Allocation	Description
Thick provisioning	QuTS hero allocates storage pool space when the shared folder is created, ensuring the space is available.
Thin provisioning	QuTS hero allocates storage pool space on demand, as data is written to the shared folder. <div style="display: flex; align-items: center;">  <div> <p>Note This option is selected by default.</p> </div> </div>

8. Optional: Click **Enable snapshot schedule and snapshot retention**.


 **Note**

By default, a snapshot is scheduled daily at 1:00 AM, and the snapshot retention policy is set to Smart Versioning. You can change these settings at any time. For details, see the following topics:

- [Configuring a Snapshot Schedule](#)
- [Configuring a Snapshot Retention Policy](#)

9. 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 (1000 TB)




Tip
Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation.

10. 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.

11. Optional: Enable folder encryption.
- Under **Folder Encryption**, click **Edit**.
 - Select **Encryption**.
Folder encryption protects folder content against unauthorized data access when the drives are physically stolen.
 - 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.

12. Click **Next**.

13. Optional: Configure any of the following storage settings.

Setting	Description
Compression	<p>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.</p> <p> Tip Compression does not impact read/write and processor performance on ZFS filesystems. Only disable this setting when necessary.</p>
Deduplication	<p>QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data.</p> <p> Important To enable deduplication your NAS must have at least 16 GB of memory.</p>
SSD cache	<p>QuTS hero adds data from this folder to the SSD cache to improve read performance.</p> <p> Important Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.</p>
Fast clone	<p>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.</p> <p> Important</p> <ul style="list-style-type: none"> • 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	<p>Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes:</p> <ul style="list-style-type: none"> • 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	<p>Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application.</p> <p> Tip The default is 64K.</p>

- 14.** 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	<p>Select a WORM type.</p> <ul style="list-style-type: none"> • 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	<p>When enabled, a file added to the folder can be modified or deleted within the lock delay time period. After this time has passed, the file automatically becomes locked and unmodifiable.</p> <p> Note</p> <ul style="list-style-type: none"> • 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.


15. Click **Next**.

16. 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](#).

17. Click **Next**.

18. 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 the kernel-mode SMB daemon is disabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	<p>Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.</p> <p> Note This option is available only when Enable Network Recycle Bin is selected.</p>
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.

19. Click **Next**.
20. Review the summary information, and then click **Finish**.

QuTS hero creates the 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: <ul style="list-style-type: none"> • 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)	<p>QuTS hero sends a notification to this email address when the account password is about to expire.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px;"> <p> Note</p> <ul style="list-style-type: none"> • 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 . </div>
(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.

	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Add to Transcode.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Select the folder. b. Click . c. Select Cancel/Delete Transcoding.
Using the context menu	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Right-click the shared folder. b. Select Lock.
Unlock the shared folder	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a. Click . b. Select Always Keep in Reserved Cache. A confirmation message appears. c. Click OK.
Using the context menu	<ol style="list-style-type: none"> 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.

Status Icon	Description
	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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

7. Storage & Snapshots

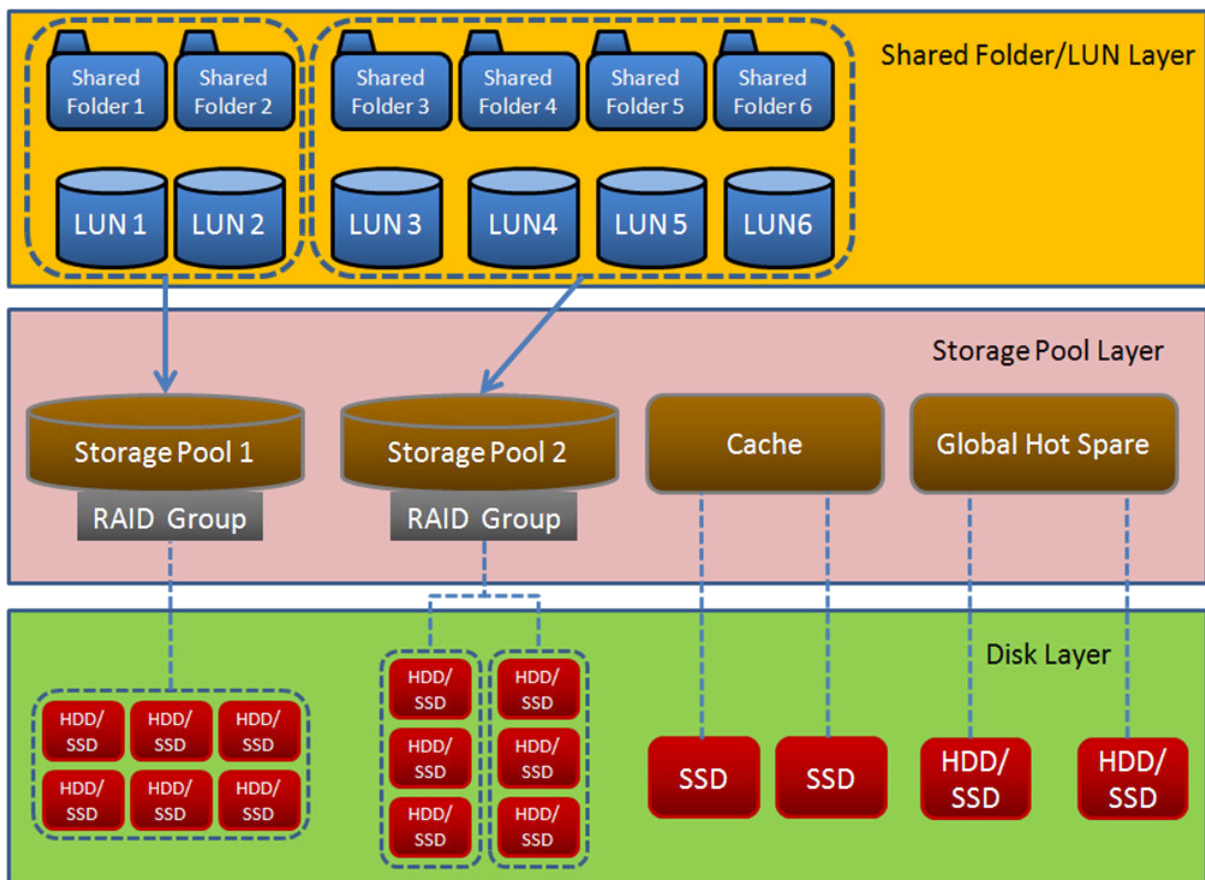
Storage & Snapshots is a QuTS hero utility that helps you create, manage, and monitor storage on your NAS. With Storage & Snapshots you can perform the following tasks:

- 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	<p>Pool scrubbing detects and automatically repairs damaged data blocks in the ZFS file system.</p> <p> Important The scrubbing task may reduce the storage pool read and write performance. You should schedule pool scrubbing to run during times of low NAS usage. You can also click Exclude Times to specify times and days of the week during which scrubbing will not run.</p>
Clean Deduplication Table	<p>When ZFS performs deduplication, it records duplicate data in a deduplication table. Cleaning removes unused entries from the deduplication table.</p> <p> Important The clean deduplication table task may reduce the system read and write performance. You should schedule this task to run during times of low NAS usage.</p>


Disk Health Global Settings

Setting	Description
Activate Predictive S.M.A.R.T. Migration	<p>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.</p>
S.M.A.R.T. polling time	<p>Specify how often QuTS hero checks disks for S.M.A.R.T. errors in minutes.</p>
Disk Temperature Alarm	<p>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.</p>

Setting	Description
TLER/ERC Timer	<p>Enable this feature to specify a maximum response time of all disks in seconds.</p> <p>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.</p> <p> Tip</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If the app DA Drive Analyzer is installed, enabling this setting sends disk analysis data that is linked to your QID to QNAP.</p> <p> Note</p> <p>Disabling this setting causes the app DA Drive Analyzer to stop working.</p>
SSD Estimated Life Warning	<p>Enable this feature to change the disk status of an SSD to "Warning" when its estimated life is lower than the specified threshold.</p>

Snapshot Global Settings

Setting	Description
Smart Snapshot Space Management	<p>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 also choose to automatically delete the most recent snapshots.</p> <p>When this feature is enabled and the snapshot retention policy is set to "Smart Versioning", the system retains the latest snapshot of each time interval when deleting snapshots. For details, see Configuring a Snapshot Retention Policy.</p> <p> Important</p> <ul style="list-style-type: none"> • If QuTS hero is unable to free at least 32GB of snapshot space, the system stops creating new snapshots. • After QuTS hero has freed more than 40GB of snapshot space, the system stops deleting old snapshots.
Enable File Station Snapshot Directory for administrators	<p>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.</p>

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	<p>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:</p> <ul style="list-style-type: none"> • Overwrite the oldest snapshot when taking a new one. • Stop taking snapshots. <p> 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.</p>
Use timezone GMT+0 for all new snapshots	<p>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.</p> <p>This setting only applies to new snapshots. Existing snapshots are not renamed.</p>
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	<p>The general health status of the disk</p> <ul style="list-style-type: none"> • 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	<p>The capacity of the disk, in both binary and decimal formats</p> <div style="border-left: 2px solid #00a0e3; padding-left: 10px;"> <p> Note</p> <ul style="list-style-type: none"> • 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). </div>
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)	<ul style="list-style-type: none"> • 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	<div style="border-left: 2px solid #e34a33; padding-left: 10px;"> <p> Important</p> <p>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.</p> </div>
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	<p>Scan the disk for bad blocks.</p> <p> Tip Run this scan if the disk's status changes to <code>Warning</code> or <code>Error</code>. If QuTS hero does not detect any bad blocks, the status changes back to <code>Ready</code>.</p> <p>To view the number of bad blocks, see Disk Health > Summary.</p>
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 Securely Erasing a Disk .
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.	<p>Click one of the following buttons:</p> <ul style="list-style-type: none"> • Test: Run an IHM test now. <p> Note The IHM test is only available for HDDs.</p> <ul style="list-style-type: none"> • 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	<p>Displays S.M.A.R.T. disk information and supported attributes.</p> <p> 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.</p>	-
Test	Run a S.M.A.R.T. disk self-test.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • 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.	<p>Configure the following settings:</p> <ul style="list-style-type: none"> • 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. <p> 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).</p>

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.

Securely Erasing a Disk

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




Important

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

1. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
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	<p>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.</p> <p>Select Customized to configure the following the erase settings.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p> Important This feature is only supported on specific SSD models.</p>
Fast	<p>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.</p>

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.

The System Pool

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



Tip

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

Creating a Storage Pool

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.
- QSAL can only be enabled when at least one SSD has over 3% estimated life remaining.

9. Click *Next*.

10. Configure any of the following settings.

Setting	Description
Optimize performance	<p>The system will optimize the pool's storage performance immediately after the pool is created.</p> <div data-bbox="592 1272 651 1330" style="float: left; margin-right: 10px;"> </div> <p>Important</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <div data-bbox="592 1727 651 1785" style="float: left; margin-right: 10px;"> </div> <p>Note</p> <p>SSD over-provisioning is automatically enabled if QNAP SSD Antiwear Leveling (QSAL) is enabled.</p>

Setting	Description
External device SSD over-provisioning	<p>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.</p> <p> Note</p> <ul style="list-style-type: none"> • This setting is available if the selected SSDs are installed in certain QNAP external device models. • This setting can only be configured for RAID types other than JBOD and RAID 0.
Pool over-provisioning	Storage pool over-provisioning reserves the specified percentage of space in the storage pool in order to maintain consistent pool access performance. Storage pool over-provisioning also extends the lifespan of SSDs in the pool.
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.

Storage Pool Management

Storage Pool Status

Status	Description
Ready	The storage pool is working normally. All RAID groups in the pool have the status <code>Ready</code> .
Warning (Degraded)	One or more RAID groups in the storage pool have the status <code>Degraded</code> . 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 <code>Degraded (Rebuilding)</code> . 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 <code>Not Active</code> .

 **Note**
It might be possible to recover some data from shared folders and LUNs.

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**.

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

Allocation	Description
Thick provisioning	QuTS hero allocates storage pool space when the shared folder is created, ensuring the space is available.
Thin provisioning	QuTS hero allocates storage pool space on demand, as data is written to the shared folder. <div style="margin-top: 10px;">  Note This option is selected by default. </div>

7. Optional: Click **Enable snapshot schedule and snapshot retention**.



Note

By default, a snapshot is scheduled daily at 1:00 AM, and the snapshot retention policy is set to Smart Versioning. You can change these settings at any time. For details, see the following topics:

- [Configuring a Snapshot Schedule](#)
- [Configuring a Snapshot Retention Policy](#)

8. 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 (1000 TB)

Tip
Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation.

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

10. 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.


11. Click **Next**.

12. Optional: Configure any of the following storage settings.

Setting	Description
Compression	<p>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.</p> <p> Tip Compression does not impact read/write and processor performance on ZFS filesystems. Only disable this setting when necessary.</p>
Deduplication	<p>QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data.</p> <p> Important To enable deduplication your NAS must have at least 16 GB of memory.</p>
SSD cache	<p>QuTS hero adds data from this folder to the SSD cache to improve read performance.</p> <p> Important Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.</p>
Fast clone	<p>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.</p> <p> Important</p> <ul style="list-style-type: none"> • 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	<p>Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes:</p> <ul style="list-style-type: none"> • 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	<p>Specify how to use the shared folder. Each option results in a different record size, optimizing performance for the specified application.</p> <p> Tip The default is 64K.</p>

- 13. 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	<p>Select a WORM type.</p> <ul style="list-style-type: none"> • 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	<p>When enabled, a file added to the folder can be modified or deleted within the lock delay time period. After this time has passed, the file automatically becomes locked and unmodifiable.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note</p> <ul style="list-style-type: none"> 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. </div>
Retention	Limit how long WORM applies to each file and folder. Files and folders can be modified after the specified time period.


14. Click **Next**.

15. 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](#).

16. Click **Next**.

17. 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 the kernel-mode SMB daemon is disabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol.
Enable Windows Previous Versions	When enabled, the Previous Versions feature in Windows can be used with the shared folder.
Enable Network Recycle Bin	Selecting this option creates a Recycle Bin for this shared folder.
Restrict the access of Recycle Bin to administrators only for now	<p>Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note</p> <p>This option is available only when Enable Network Recycle Bin is selected.</p> </div>
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.




18. Click **Next**.


19. Review the summary information, and then click **Finish**.

QuTS hero creates the shared folder.


Shared Folder Management

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

Setting	Description
Compression	<p>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.</p> <p> Tip Compression does not impact read/write and processor performance on ZFS filesystems. Only disable this setting when necessary.</p>
Deduplication	<p>QuTS hero reduces the amount of storage needed by eliminating duplicate copies of repeated data.</p> <p> Important To enable deduplication your NAS must have at least 16 GB of memory.</p>
SSD cache	<p>QuTS hero adds data from this folder to the SSD cache to improve read performance.</p> <p> Important Shared folders and LUNs created in an all-SSD storage pool cannot use the SSD cache.</p>

Setting	Description
Fast clone	<p>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.</p> <p> Important</p> <ul style="list-style-type: none"> • 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.
Synchronous I/O	<p>Select the ZFS Intent Log I/O mode to improve data consistency or performance. There are three modes:</p> <ul style="list-style-type: none"> • 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	<p>Delete the shared folder. For details, see Deleting a Shared Folder.</p>
Resize Shared Folder	<p>Change the storage capacity of a shared folder. For details, see:</p> <ul style="list-style-type: none"> • Expanding a Shared Folder • Shrinking a Shared Folder
Actions	<p>Configure the settings of the shared folder. For details, see Shared Folder Actions.</p>
View data reduction information	<p>View statistics related to compression and deduplication. For details, see Data Reduction.</p>

Shared Folder Actions

Action	Description
Edit WORM Settings	<p>Edit the WORM retention time of the folder.</p> <p> Note WORM must be enabled on the folder and set to Enterprise.</p>
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 .
Rename Shared Folder	<p>Change the name of the shared folder.</p> <ul style="list-style-type: none"> The name can be in any Unicode language. The maximum length is 64 bytes. In English, this equals 64 characters. The following special characters are not allowed: @ " + = / \ : * ? < > ; [] % , ` ' non-breaking space The last character cannot be a period (.) or space. The name cannot begin with a space or "_sn_".
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, you must modify the application to use another folder before deleting the shared folder.

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 and snapshots 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 (1000 TB)



Tip
Setting the maximum size of a shared folder to a value that is greater than the amount of free space in its parent storage pool is called over-allocation.

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	<p>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.</p> <div style="display: flex; align-items: center;">  <p>Important To enable deduplication your NAS must have at least 8 GB of memory.</p> </div>

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.	<ul style="list-style-type: none"> • Greater read/write speeds, compared to a single disk • Speeds can be increased further by adding disks 	If one disk in the RAID group fails, and the RAID group has no redundancy, all data will be lost.
Redundancy	<p>Each disk in the RAID group can store the following:</p> <ul style="list-style-type: none"> • Complete copy of the stored data • Metadata that allows reconstruction of lost data 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 5	≥ 3	1	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 Type	Number of Disks	Disk Failure Tolerance	Overview
RAID 10	≥ 4 (Must be an even number)	1 per pair of disks	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Multiple small RAID 6 groups are striped to form one RAID 60 group. • Better failure protection and faster rebuild time than RAID 6. More storage capacity than RAID 10. • Recommended if you need higher fault tolerance than RAID 50.
Triple Mirror	3	2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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**.
2. Select a storage pool.
3. Click **Manage**.
4. Select a RAID group.
5. Click **Manage**.

Action	Description
Replace Disks One By One	<p>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.</p> <p> Note You can also use this feature to replace working disks for maintenance purposes.</p>
Recover	<p>Recovers the RAID group from accidental disk removal. For details, see Recovering a RAID Group.</p>

RAID Group Status

Status	Description
Ready	The RAID group is working normally.
Degraded	One or more disks in the RAID group have failed. The number of disk failures are within the disk failure tolerance of the RAID group. There are not enough spare disks available to 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	<ul style="list-style-type: none"> • 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 <code>rebuilding</code>, and then changes back to <code>Ready</code> 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	<p>Change the SED security password. You can also choose to save the encryption key to the local NAS.</p> <p> Warning Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable.</p> <p>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.</p> <p> Warning Saving the encryption key can result in unauthorized data access if unauthorized personnel are able to physically access the NAS.</p>
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	<p>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:</p> <ul style="list-style-type: none"> • 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**.

Erasing a Disk Using SED Erase

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

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 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.

You can also perform recovery manually. 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	<p>Reset all expansion unit IDs, and then give each unit a new ID number starting from 1 based on the order that they are physically connected.</p> <p> Tip Use this action if the expansion unit IDs appear out of sequential order in the enclosure list.</p>
Attach and Recover Storage Pool	<p>Scan all free disks on the NAS and all connected expansion units for existing shared folders, LUNs, and storage pools.</p> <p> Tip Perform this action after moving disks between NAS devices.</p>

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Individual • JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10 	<ul style="list-style-type: none"> • 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. Configure pool guaranteed snapshot space.
Pool guaranteed snapshot space is storage pool space that is reserved for storing snapshots. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots.
14. Click **Next**.
15. Click **Create**.
A confirmation message appears.
16. Click **OK**.

QuTS hero creates the storage pool 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 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	<p>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.</p> <p> 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 .</p> <p> Important This button only appears when the device is in NAS Storage mode.</p>
Eject	<p>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.</p> <p> Important This button only appears when the device is in External Storage mode.</p>
Configure	<p>Create a RAID group on the RAID device and configure the storage mode.</p> <p> Important The RAID device's Mode switch must be set to Software Control mode.</p>
Check for Update	<p>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.</p>
Manage > Configure Spare Disk	<p>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.</p>
Manage > Remove	<p>Delete the RAID group. The member disks will be automatically assigned as global spare disks if the device contains any other RAID groups.</p> <p> Warning All data on the selected disks will be deleted.</p>
Manage > View Disks	<p>View the information about the disks installed in the RAID device, including their status and health information.</p> <p> Note Selecting this option takes you to the Disks/VJBOD screen.</p>

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

To view the status and health of RAID enclosures connected to the NAS, or drive adapters and the disks installed in them, go to **Storage & Snapshots > Storage > Disks/VJBOD** .

The Autoplay Menu

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

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

QNAP JBOD Enclosures

About QNAP JBOD Enclosures

QNAP JBOD enclosures are a series of expansion units designed to increase the storage capacity of your NAS, computer, or server. JBOD enclosures offer a wide range of storage applications. You can manage drives independently or group them together in a software RAID configuration using a host NAS, computer, or server. QNAP offers JBOD enclosures with USB 3.2 Gen 2 Type-C or SFF interface ports to ensure quick and efficient data transfer between the JBOD enclosure and the host device.

QNAP JBOD Enclosure Types

Enclosure Type	Description	Supported Platforms	Example Models
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: <ul style="list-style-type: none"> • QuTS hero • QTS 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Windows • Linux NAS: <ul style="list-style-type: none"> • QuTS hero • QTS 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Windows • Linux • macOS NAS: <ul style="list-style-type: none"> • QuTS hero • QTS 	<ul style="list-style-type: none"> • 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, shared folders, and RAID groups using disks installed in the JBOD enclosure.
External Storage	View and manage attached JBOD enclosures and installed disks. For details, see External Storage .

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.
Application consistent	<p>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.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>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.</p> </div>

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.

Type	Description
Application consistent	<p>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.</p> <p> 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.</p>


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


Configuring a Snapshot Retention Policy

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

 **Important**
After you create or modify a snapshot retention policy, QuTS hero applies the new policy to existing snapshots. If the new policy is more restrictive than the previous policy, 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.

Snapshot Retention Policy	UI Label	Description
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.
Smart versioning	Smart versioning	<p>Keep a snapshot created during a time period for a specified length of time. Examples:</p> <ul style="list-style-type: none"> • 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. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Important The maximum number of snapshots for all time periods combined is 256.</p> </div>

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. <div style="display: flex; align-items: center;">  <div> <p>Tip</p> <p>The default value is 20%.</p> </div> </div>
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.



Note

If a snapshot has any associated Instant Clone shared folders or LUNs, those shared folders and LUNs must be deleted before you can delete the snapshot.

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. <ul style="list-style-type: none"> • 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.
Restore	<p>Overwrite the current version of the file or folder with the previous version.</p> <div style="display: flex; align-items: center;">  <div> <p>Warning All changes made to the file or folder after the snapshot was taken will be deleted.</p> </div> </div>

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.

Regular Clone and Instant Clone

QuTS hero provides two snapshot clone methods, a regular clone method and Instant Clone. The two clone methods have different advantages and limitations.

Feature	Regular Clone	Instant Clone
Requirements	-	iSCSI service must be enabled for cloning LUNs. For details, see iSCSI & Fibre Channel Global Settings .
Cloning duration	Longer	Shorter
Required space	Normal	Less space required for cloning a thin shared folder or a thin LUN
Cloned shared folders/LUNs can be a source for Snapshot Replica jobs	Yes	No
Cloned shared folders/LUNs can be a source for SnapSync jobs	Yes	No
After cloning, you can revert to an earlier snapshot	Yes	No All Instant Clone shared folders/LUNs of the snapshot must be deleted first.
After cloning, the snapshot can be deleted	Yes	No All Instant Clone shared folders/LUNs of the snapshot must be deleted first.
After cloning, the original shared folder/LUN of the snapshot can be deleted	Yes	No All of the original shared folder/LUN's snapshots which have Instant Clone shared folders/LUNs must be deleted first.

Cloning a Shared Folder

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



Important

The shared folder 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**.
6. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).
The **Clone Snapshot** or **Instant Clone Snapshot** window opens.
7. Specify a shared folder name.
8. 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**.
6. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).
The **Clone Snapshot** or **Instant Clone Snapshot** window opens.
7. Specify a LUN name.
8. Optional: Select an iSCSI target.
QuTS hero will map the LUN copy to the target.
9. 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 <ul style="list-style-type: none"> • Member disks fail • Member disks are removed from the NAS 		✓	✓
Storage Pool Failure <ul style="list-style-type: none"> • One or more RAID groups in the pool fail • Pool is deleted 		✓	✓
NAS Hardware Failure <ul style="list-style-type: none"> • 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.
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.



Note

Shared folders and LUNs created via Instant Clone cannot be used as a source for Snapshot Replica jobs.

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	<p>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.</p> <ul style="list-style-type: none"> • Run on a schedule: The job automatically runs daily, weekly, or monthly. Settings: <ul style="list-style-type: none"> • Schedule: How often the job runs • Day: The day that the job runs on • Expiration date: The replica job stops running after this date • Frequency: How often the job runs on the days specified by "Schedule" and "Day" • Start at: The time that the job starts running. • Run once: The job runs once on a specific time and day. • Manually start: The job does not run unless a user starts it.
Take a new snapshot on a schedule, then run replication job	<p>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.</p> <ul style="list-style-type: none"> • Run on a schedule: The job automatically runs daily, weekly, or monthly. Settings: <ul style="list-style-type: none"> • 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	<p>QuTS hero encrypts the snapshot before replicating it.</p> <ul style="list-style-type: none"> • 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	<p>QuTS hero compresses snapshots when replicating them. This consumes more CPU and system memory, but reduces the amount of bandwidth required.</p> <div style="border-left: 2px solid orange; padding-left: 10px; margin-top: 10px;">  <p>Tip Enable this setting in low bandwidth networks, or if the NAS devices are connected through a WAN.</p> </div>
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 jobs and settings, go to **Storage & Snapshots > Snapshot Backup > Snapshot Replica** .

Snapshot Replica Job Actions

Icon	Description
	Enable or disable the schedule

Icon	Description
	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	<p>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.</p> <div style="display: flex; align-items: flex-start;">  <p>Warning All changes made after the snapshot was taken will be deleted.</p> </div>

Action	Description
Select Restore > Restore Files to	Choose one of the following restoration options. <ul style="list-style-type: none"> • 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 is not being accessed on the LUN. The safest way to do this is to disconnect all iSCSI initiators. Accessing the LUN during a snapshot revert might result in data loss.
- Restoration time depends on the amount of data being restored and the connection speed between the two NAS devices.

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



Important

The LUN must have at least one snapshot.

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



Warning

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

7. Optional: Configure the following settings.

Setting	Description
Take a new snapshot before reverting	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 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**.
7. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).

The **Clone Snapshot** or **Instant Clone Snapshot** window opens.

8. Specify a shared folder name.
9. Select a storage pool.
10. Optional: Select **Enable encryption during transfer**.
QuTS hero encrypts the snapshot before sending it for additional security.
11. 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**.
7. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).

The **Clone Snapshot** or **Instant Clone Snapshot** window opens.

8. Specify a LUN name.
9. Select a storage pool.
10. Optional: Select an iSCSI target.
QuTS hero will map the LUN copy to the target.
11. Select **Enable encryption during transfer**.
QuTS hero encrypts the snapshot before sending it for additional security.
12. 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**.
7. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).

The **Clone Snapshot** or **Instant Clone Snapshot** window opens.

8. Specify a shared folder name.
9. 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**.
6. Select one of the following:
 - Clone
 - Instant Clone

For details, see [Regular Clone and Instant Clone](#).
The **Clone Snapshot** or **Instant Clone Snapshot** window opens.

7. Specify a LUN name.
8. Optional: Select an iSCSI target.
QuTS hero will map the LUN copy to the target.
9. 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 a cache type.

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



Important

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

5. Click **Next**.
6. Select whether to create a read cache or a write log.



Note

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

7. Select one or more SSDs.



Warning

All data on the selected disks will be deleted.

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



Note

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



Tip

This list can be modified later.

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



Note

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



Tip

This list can be modified later.

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



Note

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

Cache Mode	Description	Recommended Use Cases
Random I/O	Only small data blocks are added to the SSD cache. Larger blocks are accessed directly from regular storage.	Virtualization, databases
All I/O	Small and large data blocks are added to the SSD cache. Both sequential and random I/O requests are accelerated.	Video streaming, large file access operations



Tip

An HDD RAID group may outperform a SSD RAID group for sequential I/O if the ratio of HDDs to SSDs is 3:1 or greater, and the HDD group has a RAID type of RAID 0, 5, 6, or 10. However, SSDs will always be faster for random I/O. If the NAS contains a RAID group of type RAID 0, 5, 6, or 10 that contains three times more disks than the SSD cache, you should select **Random I/O**.

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

Configuring SSD Cache Disks

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

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



Note

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

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



Important

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

**Warning**

All data except for system partition data will be deleted.

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

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

Configuring Cached Storage

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

**Note**

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

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

**Note**

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

**Important**

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

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

**Note**

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

6. Click **Apply**.

Removing the SSD Cache

**Note**

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

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

**Note**

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

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

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

External Storage

QuTS hero supports external USB and eSATA storage devices, such as flash drives, portable hard drives, and storage enclosures. After connecting a USB or eSATA external storage device to the NAS, the device and all of its readable partitions will be displayed in **Storage & Snapshots > Storage > External Storage** . QuTS hero will also create a shared folder for each readable partition on the device.

External Storage Device Actions

Action	Description
Erase	Delete all data and partitions on the device.
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 Disk or Partition .
Secure Erase	Permanently erase all data on a disk. For details, see Securely Erasing a Disk .



External Storage Partition Actions

Action	Description
Storage Information	Display details about the selected partition, including partition name, capacity, used space, and file system type.
Format	Format the partition. For details, see Formatting an External Storage Disk or Partition .
Encryption Management	Manage encryption on a previously encrypted device. You can lock or unlock the device, change the encryption password, or download the encryption key.
Eject	Unmount the partition. The external storage device and any stored partitions will continue working.

Formatting an External Storage Disk or Partition

1. Go to **Storage & Snapshots > Storage > External Storage** .
2. Select a disk or partition.
3. Click **Actions**, and then select **Full Disk Format** or **Format**.
The **Full Disk Format** or **Format Partition** window opens.
4. Select a file system.

File System	Recommended Operating Systems and Devices
NTFS	Windows
HTS+	macOS

File System	Recommended Operating Systems and Devices
FAT32	Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets  Important The maximum file size is 4 GB.
exFAT	Windows, macOS, some cameras, mobile phones, video game consoles, tablets  Important Verify that your device is compatible with exFAT before selecting this option.
EXT3	Linux, NAS devices
EXT4	Linux, NAS devices

5. Specify a label.

The label must consist of 1 to 16 characters from any of the following groups:

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

6. Optional: Enable encryption.

a. Select an encryption type.

Select one of the following options:

- AES 128 bits
- AES 192 bits
- AES 256 bits

b. Specify an encryption password.

The password must consist of 8 to 16 characters from any of the following groups:

- Letters: A to Z, a to z
- Numbers: 0 to 9
- All special characters (excluding spaces)

c. Confirm the encryption password.

d. Optional: Select **Save encryption key.**

Select this option to save a local copy of the encryption key on the NAS. This enables the system to automatically unlock and mount the encrypted storage space when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.



Warning

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

- If you forget the encryption password, the storage space will become inaccessible and all data will be lost.

7. Click **Format**.
A warning message appears.
8. Click **OK**.

Remote Disk

Remote disk enables 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.

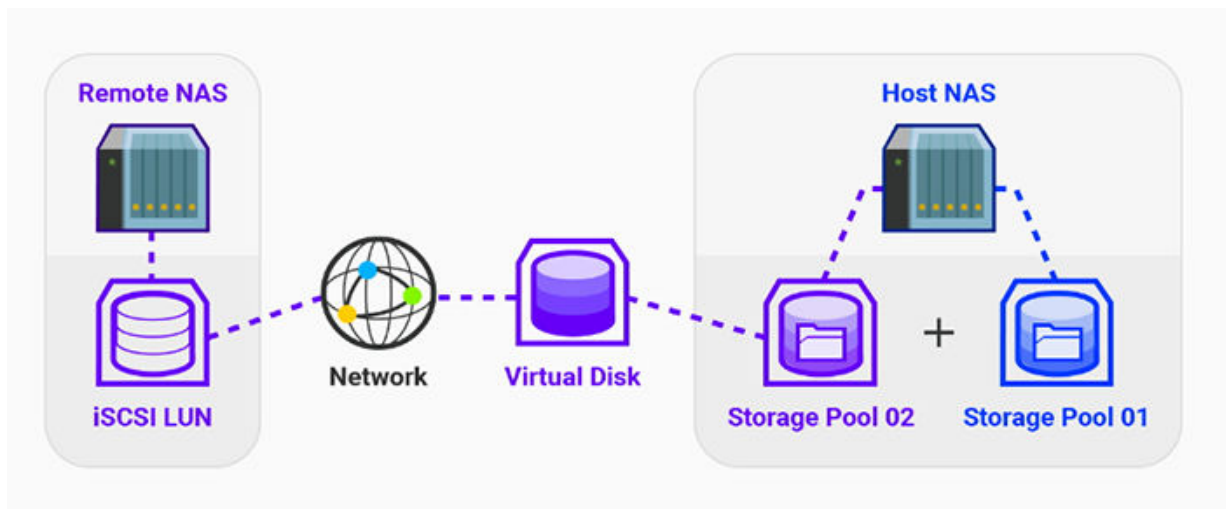
QuTS hero adds the remote disk and shares it at **Control Panel > Privilege > Shared Folders** . By default only the admin account has access.

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	<p>Format the remote disk. Select one of the following file system options:</p> <ul style="list-style-type: none"> • ext4 • ext3 • FAT32 • NTFS • HTS+ <p>Select one of the following I/O options:</p> <ul style="list-style-type: none"> • 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. <div style="margin-top: 10px;">  <p>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 <code>Virtual JBOD</code>.</p> </div>

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. <div style="margin-top: 10px;">  <p>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 <code>Virtual JBOD</code>.</p> </div>

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**.

Virtual JBOD Overview

Initiator IQN: iqn.2004-04.com.qnap:ts-x77.tw-test1 🔄 🔒 🔑 Safely Detach all

Disk Name	Status	Total Size	Local Storage Pool	Local Volume/LUN	Remote NAS	Remote Storage Pool	Remote Disk Configuration	Remote LUN Name	Connection Type
VJBOD 1	Ready	154.00 GB	-	-	TW-TEST3 (172.17.48.52)	Warning Storage Pool 1 (4.58 GB Unallocated)	RAID Group 1 RAID 0 2 Disk(s)	RemoteVJBOD1_0(E...)	TCP
					Target IQN: iqn.2004-04.com.qnap:ts-653b:iscsi:remoteyjbod1.0f93e7 (Connected)				
VJBOD 2	Ready	154.00 GB	Ready Storage Pool 1 144.50 GB	-	TW-TEST3 (172.17.48.52)	Warning Storage Pool 1 (4.58 GB Unallocated)	RAID Group 1 RAID 0 2 Disk(s)	RemoteVJBOD3_0(E...)	TCP
					Target IQN: iqn.2004-04.com.qnap:ts-653b:iscsi:remoteyjbod3.0f93e7 (Connected)				

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

- Note the details of the VJBOD disk's remote LUN.
 - Go to **Storage & Snapshots > Storage > Disks/VJBOD**.
 - Click **VJBOD**, and then select **VJBOD Overview**.
The **VJBOD Overview** window opens.
 - Locate the VJBOD disk that you want to move, and then note the **Remote LUN Name** and the IP address under **Remote NAS**.
- Detach the VJBOD disk's storage pool.
 - 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.

Installing VJBOD Cloud

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
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.	<ul style="list-style-type: none"> • 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. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Warning</p> <ul style="list-style-type: none"> • 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. </div>

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

16. Allocate stored space.
 Stored space is space used to store a copy of the volume's data locally on the NAS.

- a. Select a storage pool.
- b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the volume's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the volume's capacity	-

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

The VJBOD Cloud volume appears in the **Cloud Storage** table at **VJBOD Cloud > Overview** .

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

Creating a VJBOD Cloud LUN

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud LUN**.
The **Create VJBOD Cloud LUN** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.
For details, see [Connecting to a VJBOD Cloud Service](#).
6. Optional: Select **Use system proxy settings**.
When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel > Network & File Services > Network Access > Proxy** .
7. Click **Search**.
8. Select a cloud space.
This may be a bucket, container, account name, or something else depending on the cloud service provider.



Note

If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.

9. Optional: Click **Performance test**.
QuTS hero tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Create a new cloud LUN**.
12. Specify a LUN name.
Name requirements:
 - Length: 1-31 characters
 - Valid characters: A-Z, a-z, 0-9
 - Valid special characters: Underscore (_)
13. Specify the capacity of the LUN.
The amount of free space in the cloud storage space determines the maximum capacity.



Important

- The minimum LUN capacity is 3 GB.
- Increasing the capacity may increase cloud storage costs. Check with the cloud service provider for details.

14. Optional: Configure the sector size.

Setting	Description
Sector size	Changing the sector size to 4 KB increases LUN performance for specific applications and disk types. Important VMware does not currently support a 4 KB sector size.

15. Allocate stored space.

Stored space is space used to store a copy of the LUN's data locally on the NAS.

- a. Select a storage pool.
- b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the LUN's capacity	Additional space is needed to store metadata.
Maximum stored space capacity	2x the LUN's capacity	-

16. Click **Next**.

17. Optional: Deselect **Do not map it to a target for now**.

If deselected, the **Edit LUN Mapping** wizard appears after QuTS hero has finished creating the LUN.

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

The VJBOD Cloud LUN appears in the **Cloud Storage** table at **VJBOD Cloud > Overview** .

Reattaching an Existing VJBOD Cloud Volume



Note

When transferring a VJBOD Cloud volume from QuTS hero to QTS, ensure that all files are in subfolders. Files in the shared folder that are not in a subfolder will not be visible in QTS.

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
The **Create VJBOD Cloud Volume/LUN** window opens.
3. Click **Cloud Volume**.
The **Create VJBOD Cloud Volume** screen appears.
4. Select a cloud service.
5. Configure the selected cloud service.
Depending on the selected cloud storage provider, you may need to log in, authenticate, or configure settings through a third-party interface.

For details, see [Connecting to a VJBOD Cloud Service](#).

6. Optional: Select Use system proxy settings.

When enabled, **VJBOD Cloud** connects to the cloud storage space using the system proxy server setting, configured at **Control Panel > Network & File Services > Network Access > Proxy** .

7. Click Search.

8. Select a cloud space.

This may be a bucket, container, account name, or something else depending on the cloud service provider.



Note

If you do not have permission to browse the list of cloud spaces, then you need to enter the name of the cloud space manually.

9. Optional: Click Performance test.

QuTS hero tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.

10. Click Next.

11. Select Attach an existing cloud volume.

12. Select an existing volume.

13. Allocate stored space.

Stored space is space used to store a copy of the volume's data locally on the NAS.

- a. Select a storage pool.
- b. Specify the capacity of the stored space.

Limit	Amount	Notes
Minimum stored space capacity	1.25x the volume's capacity	Additional space is needed to store metadata.
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	<ol style="list-style-type: none"> 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. <div style="margin-top: 10px;"> <p>Note If transfer acceleration is enabled on the bucket, VJBOD Cloud automatically enables transfer acceleration on the NAS and displays a confirmation message.</p> </div>

Cloud Service	Steps
Amazon S3	<ol style="list-style-type: none"> 1. Select AmazonS3. 2. Select a cloud service: <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Select Backblaze. 2. Specify the key ID. 3. Specify the application key. 4. Optional: Select Validate SSL certificate.
Catalyst	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 1. Select GoogleCloudStorage. 2. Select OAuth. 3. Specify the project ID. 4. Optional: Select Validate SSL certificate.
HiCloud	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Select luckycloud S3. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select Validate SSL certificate.
Oracle Cloud	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Select Swift. 2. Optional: Enable keystone authentication. <ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Select Wasabi. 2. Specify the access key. 3. Specify the secret key. 4. Optional: Select Enable secure connection (SSL). 5. Optional: Select Validate SSL certificate.

VJBOD Cloud Management

You can manage VJBOD Cloud volumes and LUNs by going to **VJBOD Cloud > Overview** . Select a volume or LUN and then click **Manage**.

Volume Actions

Action	Description	Steps
Resize volume	Increase or decrease the size of the volume.	<ol style="list-style-type: none"> 1. Click Resize Volume. 2. Specify the new capacity of the volume. 3. Select the unit of storage space. 4. Optional: Click Set to Max to set the capacity of the volume equal to all free space in the cloud space. 5. Click Apply.
Utilization	View statistics showing data uploaded, data downloaded, and cache space utilization for the volume.	Click Actions , and then select Utilization .
Set Threshold	QuTS hero issues a warning notification when the percentage of used volume space is equal to or above the specified threshold.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Click Actions, and then select Check File System. 2. Click OK.
Recovery	QuTS hero periodically takes snapshots of a VJBOD Cloud volume. You can use these recovery point snapshots to restore the volume to a previous state.	For details, see Recovering a VJBOD Cloud Volume or LUN .

LUN Actions


Action	Description	Steps
Expand LUN	Increase the capacity of the LUN or its stored space.	<ol style="list-style-type: none"> 1. Click Expand LUN. 2. Specify the new capacity of the LUN or its stored space, in GB. 3. Optional: Click Set to Max to set the capacity of the LUN equal to all free space in the cloud space. 4. Click Apply.
Utilization Info	View statistics showing data uploaded, data downloaded, and cache space utilization for the LUN.	Click Actions , and then select Utilization .
Recovery	QuTS hero periodically takes snapshots of a VJBOD Cloud LUN. You can use these recovery point snapshots to restore the LUN to a previous state.	For details, see Recovering a VJBOD Cloud Volume or LUN .



Volume/LUN Connection Status

Status	Description
Ready	The cloud storage space is working normally.
Syncing	A volume or LUN is currently syncing with the cloud space.
License Expiring	The VJBOD Cloud license attached to this storage space will expire within one month. You must renew it if you want to continue using volumes and LUNs in this storage space.
License Expired	The license attached to this storage space has expired. All volumes and LUNs created in this storage space are set to read-only.
Not Ready	There is a problem with the connection to this storage space.

Volume/LUN Connection Actions

To perform one of the following actions go to **VJBOD Cloud > Overview**, select a VJBOD Cloud volume or LUN, click **Manage**, and then click **Connection**.

Action	Description
Connect	Reconnects the volume or LUN to the cloud space.
Disconnect	Disconnects the volume or LUN from the cloud space. The volume or LUN becomes read-only.
Edit	Edits the volume or LUN's cloud space connection details.
Remove	<p>Remove the volume or LUN from the NAS and delete all of its data from the cloud space.</p> <p> 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.</p>

Action	Description
Safely Detach	<p>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.</p> <p> Important</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p> Warning If Force Detach is selected, non-uploaded data stored in the volume or LUN might be deleted.</p>

Recovering a VJBOD Cloud Volume or LUN

QuTS hero periodically takes recovery point snapshots of each VJBOD Cloud volume and LUN to ensure that the volume or LUN can be recovered if it encounters an error. You can use these recovery points to restore the volume or LUN to a previous state.

1. Go to **VJBOD Cloud > Overview** .
2. Under **Cloud Storage**, select a VJBOD Cloud volume or LUN.
3. Click **Manage**.
The volume or LUN management window opens.
4. Click **Actions**, and then select **Recovery**.
The **VJBOD Cloud Volume/LUN Recovery** window opens.
5. Select a recovery point.



Warning

All changes to data made after the recovery point will be deleted.

6. Click **Recover**.

The status of the volume or LUN changes to *Recovering*, and then changes back to *ready* when the recovery process has finished.

Transfer Resources

In VJBOD Cloud, transfer resources correspond to data uploads and downloads. If VJBOD Cloud has 100 total transfer resources, that means the application can create 100 threads for uploading data to and downloading data from the cloud.

The total transfer resources allocated to VJBOD Cloud is determined by your NAS hardware. You can manage transfer resources by going to **VJBOD Cloud > Transfer Resources** .

Transfer Resource Allocation

By default, transfer resources are shared between all VJBOD Cloud volumes and LUNs. When a volume or LUN needs to upload to or download data from the cloud, VJBOD Cloud removes transfer resources from the shared transfer resource pool and temporarily allocates them to the volume or LUN, then returns them to the pool after the data transfer has finished.

A single volume or LUN may use a large number of shared transfer resources, stopping other volumes and LUNs from syncing data with the cloud. To prevent this you can reserve transfer resources for a volume or LUN, guaranteeing that those resources will always be available. You can also set a limit on the maximum number of transfer resources a volume or LUN can use.

Transfer Resource Usage Guidelines

Problem	Solution
VJBOD Cloud is taking a long time to sync data to the cloud.	Increase the total number of transfer resources allocated to VJBOD Cloud.
VJBOD Cloud is using too much NAS memory, CPU, or network bandwidth.	Decrease the total number of transfer resources allocated to VJBOD Cloud.
<ul style="list-style-type: none"> 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.

Setting	Description
Limit	<p>The maximum number of transfer resources this volume or LUN can use.</p> <p> Note To set this value, Limitation Rule must be set to <code>Limit</code>.</p>
Limitation Rule	<p>Select one of the following rules:</p> <ul style="list-style-type: none"> • Limit: The maximum number of transfer resources this volume or LUN can use is restricted. It can only use the number specified under Limit. • No Limit: The maximum number of transfer resources this volume or LUN can use is unrestricted. It can use all of its reserved resources and all shared transfer resources.

4. Click **Apply**.

Event Logs

Event logs, error messages, and warnings related to VJBOD Cloud are displayed in **VJBOD Cloud > Event Logs**. You can view logs by severity level, search logs using keywords, and configure notification settings.

Licenses

You can go to **VJBOD Cloud > Licenses** to view how many VJBOD Cloud licenses are registered to the local NAS, and how many of those licenses are currently being used. You can also purchase additional VJBOD Cloud licenses.

VJBOD Cloud Licensing Overview

VJBOD Cloud requires a license for each connection to a unique cloud space. A cloud space may be called a bucket, container, account name, or something else depending on the cloud service provider. For example, the following VJBOD Cloud volumes and LUNs require three licenses:

- *Amazon S3 → Bucket1 → Volume1*
- *Amazon S3 → Bucket2 → Volume2*
- *Azure → Space1 → LUN1*

Each unique cloud space can contain an unlimited number of VJBOD Cloud volumes and LUNs. For example, the following VJBOD Cloud volumes and LUNs require only one license:

- *Amazon S3 → Bucket1 → Volume1*
- *Amazon S3 → Bucket1 → Volume2*
- *Amazon S3 → Bucket1 → LUN1*

If a license expires, all VJBOD Cloud volumes and LUNs created from the cloud space attached to the license become read-only until the license is renewed.

VJBOD Cloud includes one free license.

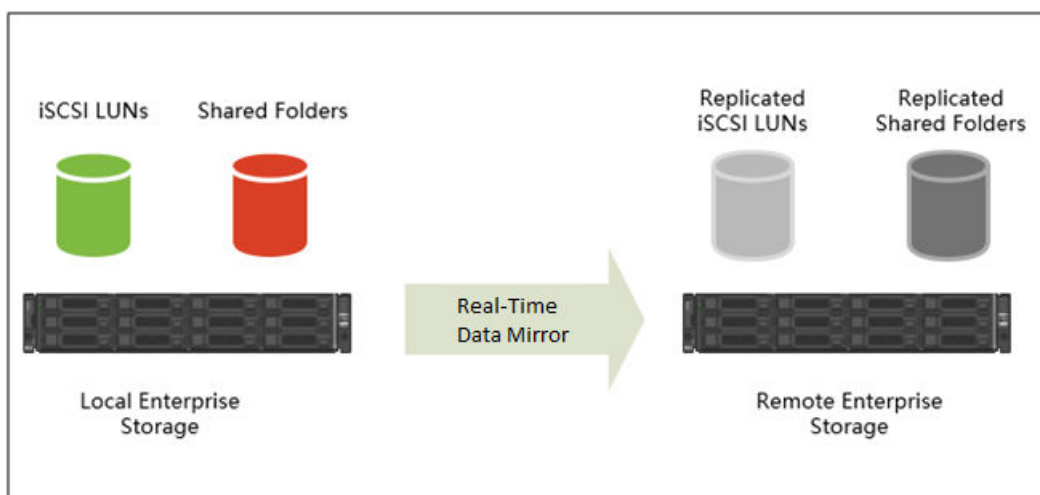
Purchasing VJBOD Cloud Licenses

1. Go to **VJBOD Cloud > Licenses**.

2. Click **Purchase License**.
The **License Center** window opens.
3. Click **Software Store**.
4. Locate **VJBOD Cloud**, and then click **Buy**.
5. Follow the onscreen instructions to purchase and activate the VJBOD Cloud licenses.

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 versions 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	<ul style="list-style-type: none"> • 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.



Note

Shared folders and LUNs created via Instant Clone cannot be used as a source for SnapSync jobs.

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.
Support application consistent snapshots	<p>SnapSync creates application consistent snapshots.</p> <p> 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.</p>

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	<p>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.</p> <p> Note The adapter lists are automatically filtered to only display adapters that can connect to the currently selected adapter.</p>

20. Click **Next**.

21. Configure the latency monitor.

Latency Monitor monitors the latency of the SnapSync job to ensure the job is running normally. If the job latency goes over the threshold six times within a minute, QuTS hero issues a warning notification.

- a. Enable **Latency threshold**.
- b. Set a threshold value, in milliseconds. The value must be 1–5000.



Tip

To determine the threshold value, run a SnapSync performance test by clicking **Create a Performance Test**. To view the average latency in previous performance tests, click **Performance Report**.

22. Click **Next**.

- 23. Optional: Select **Execute backup immediately**.
When selected, the job will run immediately after it has been created.
- 24. 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.



Note

Shared folders and LUNs created via Instant Clone cannot be used as a source for SnapSync jobs.

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.

Backup Plan	Description
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	<p>SnapSync creates application consistent snapshots.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> 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.</p> </div>

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.

Adapter Setting	Description
Manual-Select Network Adapter	<p>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.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note The adapter lists are automatically filtered to only display adapters that can connect to the currently selected adapter. </div>

20. Click **Next**.

21. Configure the latency monitor.

Latency Monitor monitors the latency of the SnapSync job to ensure the job is running normally. If the job latency goes over the threshold six times within a minute, QuTS hero issues a warning notification.

- a. Enable **Latency threshold**.
- b. Set a threshold value, in milliseconds. The value must be 1–5000.



Tip

To determine the threshold value, run a SnapSync performance test by clicking **Create a Performance Test**. To view the average latency in previous performance tests, click **Performance Report**.

22. Click **Next**.

23. Optional: Select **Execute backup immediately**.

When selected, the job will run immediately after it has been created.

24. Click **Create**.

SnapSync Management

You can manage SnapSync by going 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.
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.