



QNAP

QTS 4.5.x

User Guide



Document Version: 5
23/04/2021

Contents

1. Overview

| | |
|--|----|
| About QTS..... | 11 |
| What's New in QTS..... | 11 |
| Support and Other Resources..... | 12 |
| NAS Access..... | 13 |
| Accessing the NAS Using a Browser..... | 13 |
| Accessing the NAS Using Qfinder Pro..... | 14 |
| Accessing the NAS Using Qmanager..... | 14 |
| 2-step Verification..... | 15 |
| QTS Navigation..... | 17 |
| Task Bar..... | 17 |
| Main Menu..... | 24 |
| Desktop..... | 26 |
| Getting Started..... | 30 |

2. System Settings

| | |
|---|----|
| General Settings..... | 32 |
| Configuring System Administration Settings..... | 32 |
| Configuring Time Settings..... | 33 |
| Configuring Daylight Saving Time..... | 34 |
| Configuring Codepage Settings..... | 35 |
| Configuring Region Settings..... | 35 |
| Configuring the Login Screen..... | 35 |
| Enabling or Disabling Console Management..... | 36 |
| Security..... | 36 |
| Configuring the Allow/Deny List..... | 36 |
| Configuring IP Access Protection..... | 37 |
| Configuring Account Access Protection..... | 38 |
| SSL Certificate & Private Key..... | 38 |
| Configuring the Password Policy..... | 39 |
| Hardware..... | 40 |
| Configuring General Hardware Settings..... | 40 |
| Configuring Audio Alert Settings..... | 41 |
| Configuring Smart Fan Settings..... | 41 |
| Configuring Hardware Resource Settings..... | 42 |
| Viewing Single Root I/O Virtualization (SR-IOV) Settings..... | 43 |
| Power..... | 44 |
| EuP Mode..... | 44 |
| Wake-on-LAN (WOL)..... | 44 |
| Power Recovery..... | 44 |
| Power Schedule..... | 45 |
| Firmware Update..... | 45 |
| Firmware Update Requirements..... | 46 |
| Checking for Live Updates..... | 46 |
| Updating the Firmware Manually..... | 47 |
| Updating the Firmware Automatically..... | 48 |
| Updating the Firmware Using Qfinder Pro..... | 49 |
| Backup/Restore..... | 50 |
| Backing Up System Settings..... | 50 |
| Restoring System Settings..... | 50 |
| System Reset and Restore to Factory Default..... | 50 |

| | |
|---|----|
| External Device..... | 54 |
| USB Printer..... | 54 |
| Uninterruptible Power Supply (UPS)..... | 55 |
| NAS Behavior During a Power Outage..... | 55 |
| Configuring the UPS Settings..... | 56 |
| System Status..... | 57 |
| Resource Monitor..... | 57 |

3. Privilege Settings

| | |
|--|-----|
| Users..... | 59 |
| Default Administrator Account..... | 59 |
| Creating a Local User..... | 61 |
| Creating Multiple Users..... | 63 |
| User Account Lists..... | 64 |
| Importing Users..... | 65 |
| Exporting Users..... | 66 |
| Modifying User Account Information..... | 67 |
| Deleting Users..... | 68 |
| Home Folders..... | 68 |
| User Groups..... | 69 |
| Default User Groups..... | 69 |
| Creating a User Group..... | 69 |
| Modifying User Group Information..... | 70 |
| Deleting User Groups..... | 71 |
| Shared Folders..... | 72 |
| Default Shared Folders..... | 72 |
| Creating a Shared Folder..... | 72 |
| Editing Shared Folder Properties..... | 75 |
| Refreshing a Shared Folder..... | 78 |
| Removing Shared Folders..... | 78 |
| Enabling Daily Updates for Shared Folders..... | 78 |
| Snapshot Shared Folders..... | 78 |
| ISO Shared Folders..... | 81 |
| Shared Folder Permissions..... | 83 |
| Folder Aggregation..... | 86 |
| Shared Folder Encryption..... | 89 |
| Shared Folder Access..... | 91 |
| Quota..... | 96 |
| Enabling Quotas..... | 97 |
| Editing Quota Settings..... | 97 |
| Exporting Quota Settings..... | 98 |
| Quota Conflicts..... | 98 |
| Domain Security..... | 98 |
| Active Directory (AD) Authentication..... | 99 |
| Azure Active Directory Single Sign-On (SSO)..... | 101 |
| LDAP Authentication..... | 103 |
| AD and LDAP Management..... | 104 |
| Domain Controller..... | 106 |
| Enabling a Domain Controller..... | 106 |
| Resetting a Domain Controller..... | 107 |
| Default Domain User Accounts..... | 107 |
| Creating a Domain User..... | 108 |
| Creating Multiple Domain Users..... | 109 |
| Domain User Account Lists..... | 110 |
| Modifying Domain User Account Information..... | 111 |
| Deleting Domain Users..... | 112 |
| Domain User Groups..... | 113 |

| | |
|----------------------|-----|
| Computers..... | 114 |
| DNS..... | 116 |
| Back Up/Restore..... | 119 |

4. Services

| | |
|----------------------------------|-----|
| Antivirus..... | 120 |
| Enabling Antivirus..... | 120 |
| Scanning Shared Folders..... | 120 |
| Managing Scan Jobs..... | 122 |
| Managing Reported Scan Jobs..... | 122 |
| Managing Quarantine Files..... | 123 |
| Servers..... | 124 |
| Web Server..... | 124 |
| Enabling LDAP Server..... | 127 |
| SQL Server..... | 128 |
| Syslog Server..... | 129 |
| RADIUS Server..... | 131 |
| Enabling TFTP Server..... | 134 |
| Enabling NTP Server..... | 134 |

5. File Station

| | |
|---|-----|
| Overview..... | 136 |
| About File Station..... | 136 |
| System Requirements..... | 136 |
| Supported File Formats..... | 136 |
| Parts of the User Interface..... | 137 |
| Settings..... | 140 |
| File Operations..... | 143 |
| Uploading a File..... | 144 |
| Downloading a File..... | 145 |
| Opening a File..... | 145 |
| Opening Microsoft Word, Excel, and PowerPoint Files Using the Chrome Extension..... | 146 |
| Opening a Text File Using Text Editor..... | 146 |
| Viewing a File in Google Docs..... | 147 |
| Viewing a File in Microsoft Office Online..... | 147 |
| Opening Image Files Using Image2PDF..... | 148 |
| Viewing File Properties..... | 148 |
| Modifying File Permissions..... | 149 |
| Sorting Files..... | 150 |
| Copying a File..... | 150 |
| Moving a File..... | 151 |
| Renaming a File..... | 153 |
| Deleting a File..... | 153 |
| Restoring a Deleted File..... | 154 |
| Mounting an ISO File..... | 154 |
| Unmounting an ISO File..... | 155 |
| Compressing a File..... | 155 |
| Extracting Compressed Files or Folders..... | 156 |
| Sharing a File or Folder by Email..... | 156 |
| Sharing a File or Folder on a Social Network..... | 159 |
| Sharing a File or Folder Using Share Links..... | 160 |
| Sharing a File or Folder with a NAS User..... | 162 |
| Playing an Audio File..... | 164 |
| Playing a Video File..... | 164 |
| Playing a Video File Using CAYIN MediaSign Player..... | 165 |
| Opening a 360-degree Image or Video File..... | 165 |

| | |
|--|-----|
| Streaming to a Network Media Player..... | 166 |
| Adding a File to the Transcoding Folder..... | 166 |
| Canceling or Deleting Transcoding..... | 167 |
| Viewing Transcode Information..... | 168 |
| Folder Operations..... | 168 |
| Uploading a Folder..... | 169 |
| Uploading a Folder Using Drag and Drop..... | 169 |
| Viewing Folder Properties..... | 170 |
| Viewing Storage Information..... | 171 |
| Modifying Folder Permissions..... | 171 |
| Viewing Qsync Folders..... | 172 |
| Managing Share Links..... | 173 |
| Viewing Files and Folders Shared with Me..... | 173 |
| Creating a Folder..... | 173 |
| Copying a Folder..... | 174 |
| Creating a Desktop Shortcut..... | 174 |
| Adding a Folder to Favorites..... | 175 |
| Removing a Folder from Favorites..... | 175 |
| Compressing a Folder..... | 176 |
| Deleting a Folder..... | 177 |
| Creating a Shared Folder..... | 177 |
| Creating a Snapshot Shared Folder..... | 179 |
| Sharing Space with a New User..... | 181 |
| Adding a Folder to the Transcoding Folder..... | 181 |
| Canceling or Deleting Transcoding..... | 182 |
| Locking or Unlocking an Encrypted Shared Folder..... | 183 |
| Keeping a Folder or a File in Reserved Cache..... | 183 |
| Removing a Folder from Reserved Cache..... | 184 |

6. Storage & Snapshots

| | |
|--|-----|
| QTS Flexible Volume Architecture..... | 186 |
| Global Settings..... | 187 |
| Storage Global Settings..... | 187 |
| Disk / Device Global Settings..... | 188 |
| Snapshot Global Settings..... | 189 |
| Storage..... | 190 |
| Disks..... | 190 |
| Volumes..... | 196 |
| Storage Pools..... | 212 |
| RAID..... | 219 |
| Self-Encrypting Drives (SEDs)..... | 228 |
| Expansion Units..... | 234 |
| Expansion Unit Actions..... | 234 |
| Expansion Unit Automatic Recovery..... | 235 |
| QNAP External RAID Devices..... | 235 |
| QNAP JBOD Enclosures..... | 249 |
| Qtier..... | 251 |
| Qtier Benefits..... | 251 |
| Qtier Requirements..... | 253 |
| Qtier Creation..... | 253 |
| Qtier Management..... | 257 |
| Tiering On Demand..... | 261 |
| Snapshots..... | 261 |
| Snapshot Storage Limitations..... | 261 |
| Snapshot Creation..... | 262 |
| Snapshot Management..... | 263 |
| Snapshot Data Recovery..... | 266 |

| | |
|---|-----|
| Snapshot Clone..... | 268 |
| Snapshot Replica..... | 269 |
| Cache Acceleration..... | 280 |
| Cache Acceleration Requirements..... | 280 |
| Creating the SSD Cache..... | 280 |
| Expanding the SSD Cache..... | 282 |
| Configuring SSD Cache Settings..... | 282 |
| Cache Missing..... | 283 |
| Removing the SSD Cache..... | 284 |
| External Storage..... | 284 |
| External Storage Device Actions..... | 284 |
| External Storage Disk Actions..... | 284 |
| External Storage Partition Actions..... | 284 |
| Formatting an External Storage Partition..... | 285 |
| Remote Disk..... | 286 |
| Remote Disk Limitations..... | 286 |
| Adding a Remote Disk..... | 286 |
| Remote Disk Actions..... | 288 |
| VJBOD (Virtual JBOD)..... | 288 |
| VJBOD Requirements..... | 289 |
| VJBOD Limitations..... | 289 |
| VJBOD Automatic Reconnection..... | 290 |
| VJBOD Creation..... | 290 |
| VJBOD Management..... | 294 |
| VJBOD Cloud..... | 297 |
| Installation..... | 297 |
| VJBOD Cloud Volume and LUN Creation..... | 297 |
| Overview..... | 309 |
| Transfer Resources..... | 313 |
| Event Logs..... | 314 |
| Licenses..... | 315 |

7. iSCSI & Fibre Channel

| | |
|--|-----|
| Storage Limits..... | 317 |
| iSCSI Storage Limits..... | 317 |
| Fibre Channel Storage Limits..... | 317 |
| iSCSI & Fibre Channel Global Settings..... | 317 |
| LUNs..... | 317 |
| QTS LUN Types..... | 317 |
| Creating a Block-Based LUN..... | 318 |
| Creating a File-Based LUN..... | 320 |
| iSCSI..... | 321 |
| Getting Started with iSCSI..... | 321 |
| iSCSI Performance Optimization..... | 322 |
| iSCSI Storage..... | 322 |
| Fibre Channel..... | 331 |
| FC Ports..... | 331 |
| FC Storage..... | 334 |
| FC WWPN Aliases..... | 336 |
| LUN Import/Export..... | 338 |
| Creating a LUN Export Job..... | 338 |
| Importing a LUN from an Image File..... | 340 |
| LUN Import/Export Job Actions..... | 341 |
| LUN Import/Export Job Status..... | 341 |

8. SSD Profiling Tool

| | |
|---|-----|
| SSD Over-Provisioning..... | 342 |
| SSD Extra Over-Provisioning..... | 342 |
| SSD Over-Provisioning Tests..... | 342 |
| Creating an SSD Over-Provisioning Test..... | 342 |
| Review..... | 343 |
| Test Reports..... | 344 |
| Test Report Actions..... | 344 |
| Test Report Information..... | 345 |
| Settings..... | 345 |

9. Hybrid Backup Sync

| | |
|-------------------------------------|-----|
| About Hybrid Backup Sync..... | 346 |
| Configuring HBS 3 Settings..... | 346 |
| Jobs..... | 347 |
| Backup Jobs..... | 347 |
| Restore Jobs..... | 364 |
| Sync Jobs..... | 371 |
| Job Management..... | 389 |
| Job Reports..... | 391 |
| Incoming Jobs..... | 393 |
| Services..... | 393 |
| Time Machine..... | 393 |
| Rsync Server..... | 394 |
| RTRR Server..... | 395 |
| Configuring USB One Touch Copy..... | 397 |
| Storage Spaces..... | 398 |
| Storage Space Creation..... | 398 |
| Editing a Storage Space..... | 417 |
| Deleting a Storage Space..... | 417 |

10. Network & Virtual Switch

| | |
|--|-----|
| About Network & Virtual Switch..... | 418 |
| Basic and Advanced Mode..... | 418 |
| Overview..... | 418 |
| Interfaces..... | 418 |
| IP Address..... | 419 |
| DNS..... | 421 |
| Virtual LANs (VLANs)..... | 422 |
| Port Trunking..... | 423 |
| System Default Gateway..... | 424 |
| USB QuickAccess..... | 425 |
| Wi-Fi..... | 426 |
| Thunderbolt..... | 436 |
| Virtual Switches..... | 438 |
| Creating a Virtual Switch in Basic Mode..... | 439 |
| Creating a Virtual Switch in Advanced Mode..... | 439 |
| Creating a Virtual Switch in Software-defined Switch Mode..... | 442 |
| DHCP Server | 443 |
| Creating a DHCP Server | 443 |
| DHCP Clients..... | 446 |
| RADVD..... | 446 |
| Route..... | 449 |
| Creating a Static Route..... | 450 |
| DDNS..... | 450 |
| Adding a DDNS Service..... | 451 |

11. Network & File Services

| | |
|--|-----|
| Network Access..... | 452 |
| Service Binding..... | 452 |
| Proxy Server..... | 452 |
| Service Ports..... | 453 |
| Win/Mac/NFS..... | 454 |
| Microsoft Networking..... | 454 |
| Apple Networking..... | 456 |
| NFS Service..... | 457 |
| Telnet/SSH..... | 457 |
| Configuring Telnet Connections..... | 457 |
| Configuring SSH Connections..... | 457 |
| Editing SSH Access Permissions..... | 458 |
| SNMP..... | 458 |
| Configuring SNMP Settings..... | 458 |
| SNMP Management Information Base (MIB)..... | 459 |
| Service Discovery..... | 460 |
| UPnP Discovery Service..... | 460 |
| Bonjour..... | 460 |
| FTP..... | 460 |
| Configuring FTP Settings..... | 460 |
| Configuring Advanced FTP Settings..... | 461 |
| Network Recycle Bin..... | 462 |
| Configuring the Network Recycle Bin..... | 462 |
| Deleting All Files in the Network Recycle Bin..... | 462 |
| Restricting Access to the Network Recycle Bin..... | 462 |

12. myQNAPcloud

| | |
|--|-----|
| Getting Started..... | 464 |
| Account Setup..... | 464 |
| Creating a QNAP ID With Email or Phone Number..... | 464 |
| Registering a Device to myQNAPcloud..... | 465 |
| Installing myQNAPcloud Link..... | 466 |
| Overview..... | 466 |
| Configuring Port Forwarding..... | 467 |
| Configuring DDNS Settings..... | 467 |
| Restarting DDNS Service..... | 468 |
| Configuring Published Services..... | 468 |
| Enabling myQNAPcloud Link..... | 469 |
| Configuring Device Access Controls..... | 469 |
| Installing an SSL Certificate..... | 470 |

13. App Center

| | |
|--|-----|
| Overview..... | 472 |
| Left Panel..... | 472 |
| Toolbar..... | 472 |
| Main Area..... | 473 |
| App Management..... | 474 |
| Viewing App Information..... | 474 |
| Subscribing to an App License..... | 474 |
| Installing an App from App Center..... | 475 |
| Installing an App Manually..... | 475 |
| Updating an App..... | 476 |
| Batch Updating Multiple Apps..... | 476 |
| Enabling or Disabling an App..... | 477 |

| | |
|---|-----|
| Migrating an App..... | 477 |
| Granting or Denying User Access to an App..... | 478 |
| Uninstalling an App..... | 478 |
| App Center Settings..... | 478 |
| Adding an App Repository..... | 478 |
| Configuring App Update Settings..... | 479 |
| Digital Signatures..... | 479 |
| Enabling Installation of Apps without Digital Signatures..... | 480 |

14. Licenses

| | |
|--|-----|
| About QNAP Licenses..... | 481 |
| License Types and Plans..... | 481 |
| Validity Period..... | 481 |
| License Portals and Utility..... | 482 |
| Software Store..... | 482 |
| License Center..... | 482 |
| License Manager..... | 482 |
| Buying a License Using QNAP ID..... | 483 |
| License Activation..... | 484 |
| Activating a License Using QNAP ID..... | 484 |
| Activating a License Using a License Key..... | 486 |
| Activating a License Using a Product Key or PAK..... | 487 |
| Activating a License Offline..... | 488 |
| License Deactivation..... | 489 |
| Deactivating a License Using QNAP ID..... | 490 |
| Deactivating a License Offline..... | 490 |
| License Extension..... | 491 |
| Extending a License Using QNAP ID..... | 492 |
| Extending a License Offline Using an Unused License..... | 492 |
| Extending a License Offline Using a Product Key..... | 494 |
| Upgrading a License..... | 495 |
| Viewing License Information..... | 496 |
| Recovering Licenses..... | 497 |
| Transferring a License to the New QNAP License Server..... | 497 |
| Deleting a License..... | 498 |

15. Multimedia

| | |
|---|-----|
| HybridDesk Station (HD Station)..... | 499 |
| Installing HD Station..... | 500 |
| Configuring HD Station..... | 501 |
| HD Station Applications..... | 502 |
| Using HD Player in HD Station..... | 502 |
| HDMI Local Display and DLNA Media Server..... | 502 |
| Enabling HDMI Display Applications..... | 502 |
| Enabling DLNA Media Server..... | 503 |
| Configuring DLNA Media Server..... | 503 |
| Media Streaming Add-on..... | 503 |
| Configuring General Settings..... | 504 |
| Configuring Browsing Settings..... | 505 |
| Configuring Media Receivers..... | 505 |
| Multimedia Console..... | 506 |
| Overview..... | 506 |
| Content Management..... | 507 |
| Indexing..... | 507 |
| Thumbnail Generation..... | 508 |
| Transcoding..... | 511 |

| | |
|--|-----|
| Multimedia App Suite..... | 516 |
| Installing and Managing AI Engines | 518 |

16. QuLog Center

| | |
|--|-----|
| Monitoring System Logs..... | 520 |
| System Event Log..... | 520 |
| Monitoring System Access Logs..... | 520 |
| Local Logs..... | 521 |
| Local System Event Logs..... | 521 |
| Local System Access Logs..... | 524 |
| Viewing Online Users..... | 526 |
| Creating a Custom Filter Tab for Local Device System Logs..... | 526 |
| Local Log Settings..... | 529 |
| QuLog Service..... | 533 |
| Configuring Log Sender Settings..... | 533 |
| Configuring Log Receiver Settings..... | 534 |
| Viewing and Managing Remote Logs..... | 537 |
| Notification Settings..... | 546 |
| Configuring Notification Rule Settings..... | 546 |
| Adding a Log Filter..... | 547 |
| Editing a Log Filter..... | 548 |
| Removing a Log Filter..... | 548 |

17. Notification Center

| | |
|---|-----|
| Overview..... | 549 |
| Notification Queue and History..... | 549 |
| Queue..... | 549 |
| History..... | 549 |
| Service Account and Device Pairing..... | 550 |
| Email Notifications..... | 551 |
| SMS Notifications..... | 553 |
| Instant Messaging Notifications..... | 555 |
| Push Notifications..... | 557 |
| System Notification Rules..... | 559 |
| Managing Event Notification Rules..... | 559 |
| Alert Notifications..... | 563 |
| Settings..... | 566 |
| Enabling Send Notification Data to QNAP..... | 567 |
| Disabling Send Notification Data to QNAP..... | 567 |
| Global Notification Settings..... | 568 |
| System Logs..... | 568 |

18. Malware Remover

| | |
|----------------------------------|-----|
| About Malware Remover..... | 570 |
| Overview..... | 570 |
| Running a Malware Scan..... | 570 |
| Running a Scheduled Scan..... | 571 |
| Settings..... | 571 |
| Configuring Malware Remover..... | 571 |

19. Helpdesk

| | |
|---------------------------|-----|
| Overview..... | 573 |
| Configuring Settings..... | 573 |
| Help Request..... | 573 |
| Submitting a Ticket..... | 574 |
| Remote Support..... | 575 |

| | |
|-------------------------------------|-----|
| Enabling Remote Support..... | 575 |
| Extending Remote Support..... | 575 |
| Disabling Remote Support..... | 575 |
| Diagnostic Tool..... | 576 |
| Downloading Logs..... | 576 |
| Performing an HDD Standby Test..... | 576 |
| Performing an HDD Stress Test..... | 576 |

20. Console Management

| | |
|---|-----|
| Enabling Secure Shell (SSH)..... | 577 |
| Enabling SSH on the NAS..... | 577 |
| Enabling SSH on the NAS Using Qfinder Pro..... | 577 |
| Accessing Console Management..... | 577 |
| Accessing Console Management from Windows..... | 577 |
| Accessing Console Management from Mac..... | 578 |
| Logging In to Console Management..... | 578 |
| Managing Existing Applications..... | 578 |
| Activating or Deactivating a License..... | 579 |
| Sorting and Filtering System Logs..... | 580 |
| Showing Network Settings..... | 582 |
| Restoring or Reinitializing the Device..... | 582 |
| Rebooting the NAS..... | 582 |
| Rebooting the Device Into Rescue Mode..... | 582 |
| Rebooting the Device Into Maintenance Mode..... | 583 |

1. Overview

About QTS

QTS is a Linux-based operating system that runs applications for file management, virtualization, surveillance, multimedia, and other purposes. The optimized kernel and various services efficiently manage system resources, support applications, and protect your data. QTS also has built-in utilities that extend the functionality and improve the performance of the NAS.

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

What's New in QTS

| Version | Major New Features and Enhancements |
|-----------|--|
| QTS 4.5.3 | <ul style="list-style-type: none"> • QTS now supports a maximum of 4TB SSD cache on ARM 64-bit models. • QTS now supports up to 100,000 shared links for files or folders. • Users in the administrator group can now manage all shared links. • App Center now automatically installs required updates by default. • Added support for customizing the HTTP response header "Server". • Added support for using SNMP with IPv6. • Improved the user interface design for QTS web installation. • To enhance device security, QTS now automatically checks SQL Server password and disables the service if users still use the default password. Web Server service is now disabled by default. |
| QTS 4.5.2 | <ul style="list-style-type: none"> • QTS now supports single-root input/output virtualization (SR-IOV) and automatically displays SR-IOV device information if your NAS model and expansion card both support SR-IOV. • QTS now supports QuFirewall, a firewall utility that monitors and controls network traffic to protect the NAS from malicious cyber attacks. • Storage & Snapshots now supports displaying the supported bus types of SSD slots. • Network & Virtual Switch now supports auto-negotiation between various network speeds (1 GbE, 2.5 GbE, 5 GbE, 10 GbE) for the Intel X550 network adapter to provide backward compatibility. • Users can now enable or disable Console Management in Control Panel. • Users can now manually specify a bucket name when creating a cloud volume/LUN if their privileges do not allow for browsing the bucket list. • Increased the maximum number of local users to 16000. • Added support for the TR-10xCT series. |

| Version | Major New Features and Enhancements |
|-----------|---|
| QTS 4.5.1 | <ul style="list-style-type: none"> • QTS now supports QuLog Center, which replaces System Logs and allows for centralized log management of system events, system access, and online user status on your devices. • Hybrid Backup Sync 3 (HBS 3) now replaces Backup Station as the built-in backup application. • QTS now provides Console Management, a command-line interface that supports log viewing, app management, license activation, and other operations via SSH. • QTS now supports TL series SAS JBOD enclosures. • QTS now indicates whether a device supports Intel QuickAssist Technology. • Virtualization Station now supports live migration. Users can now migrate a running virtual machine while ensuring the continuity of services. • Storage & Snapshots now supports displaying disk health information for Seagate IronWolf SSDs in Seagate IHM (IronWolf Health Management). • Added support for joining the NAS (x86 models) to Azure Active Directory Domain Service via site-to-site VPN. |

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/en/nas-migration |
| Expansion Unit Compatibility | http://www.qnap.com/go/compatibility-expansion |
| Service Portal | https://service.qnap.com |
| Product Support Status | https://www.qnap.com/en/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 |
| Explorer (Windows) | <p>You can map a NAS shared folder as a network drive to easily access files using Explorer.</p> <p>For details on mapping shared folders, see Mapping a Shared Folder on a Windows Computer.</p> | <ul style="list-style-type: none"> Windows computer that is connected to the same network as the NAS Qfinder Pro |
| Finder (macOS) | <p>You can mount a NAS shared folder as a network drive to easily access files using Finder.</p> <p>For details on mounting shared folders, see Mounting a Shared Folder on a Mac Computer.</p> | <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 QTS login screen appears.

4. Optional: Log in QTS using HTTPS.
 - a. Select **Secure login**.
A confirmation message appears.
 - b. Click **OK**.
You will be redirected to the QTS HTTPS login page.
5. Specify your username and password.
6. Click **Login**.
The QTS desktop appears.

Accessing the NAS Using Qfinder Pro

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



Tip

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

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

Accessing the NAS Using Qmanager

1. Install Qmanager on an Android or iOS device.



Tip

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

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

| Action | Steps |
|-------------------|--|
| Add NAS manually | <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). QTS 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.
QTS 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 QTS, 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 QTS Using 2-step Verification

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




Disabling 2-step Verification



| Situation | User Action | Steps |
|--|--|---|
| Users are locked out of their accounts. | Administrators can disable 2-step verification from the Control Panel. | <ol style="list-style-type: none"> 1. Go to Control Panel > Privilege > Users . 2. Identify a locked out user, and then click . 3. Deselect 2-step Verification. 4. Click OK. |
| An administrator is locked out and no other administrators can access the account. | An administrator must restore the factory settings. | <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> |

QTS Navigation

Task Bar



| No. | Element | Possible User Actions |
|-----|---|---|
| 1 | Show Desktop | Click the button to minimize or restore all open windows. |
| 2 | Main Menu | Click the button to open the Main Menu panel on the left side of the desktop. |
| 3 | Search | <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. If the application is not yet installed, QTS opens the corresponding download screen in the App Center window. <p> Tip App or utility search results are classified into Systems, Application, and Help.</p> |
| 4 | Volume Control  Important This feature is only available on models with certain hardware specifications. | Click the button to view the following: <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 | Background Tasks | <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. |

| No. | Element | Possible User Actions |
|-----|----------------------------|---|
| 6 | External Devices | <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 | Event Notifications | <ul style="list-style-type: none"> • Hover the mouse pointer over the button to see the number of recent errors, warnings, and notices. • Click the button to view the following details for each event: <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 | Options | Click your profile picture to open the Options screen. |
| 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 QTS 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 QTS 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 volume name |
| 11 | Dashboard | Click the button to display the dashboard. |

Options

Options

— ×

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



Username: **admin**

E-mail:

Phone number:

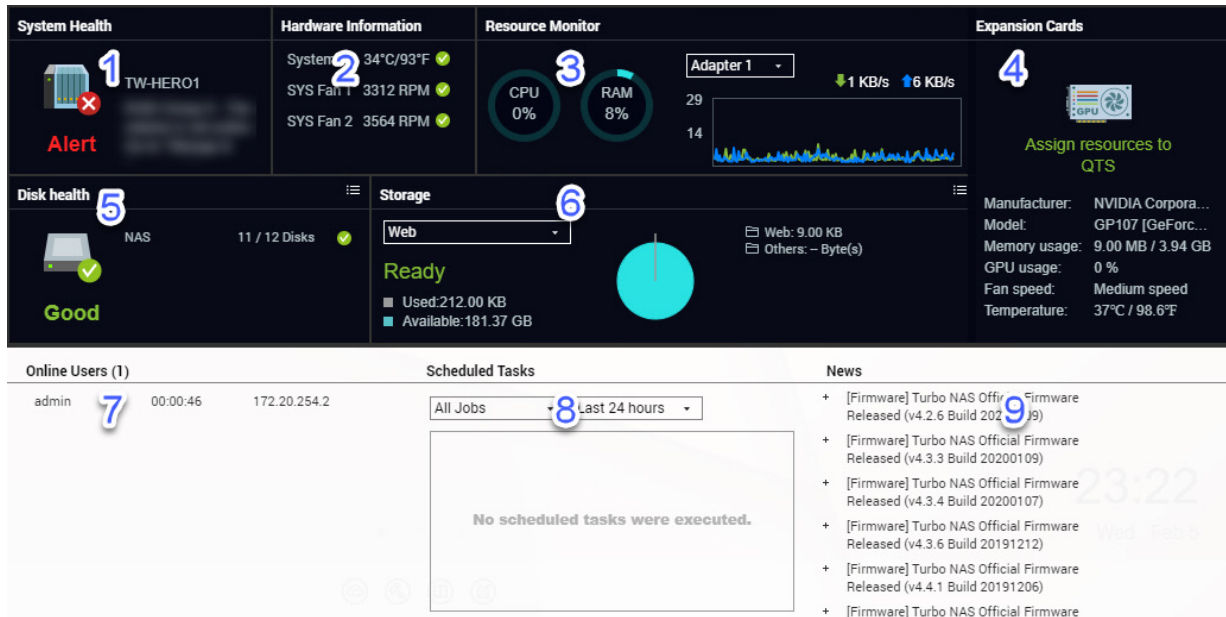
System Access Log: [View](#)

[Edit login screen](#)

| 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 | <ul style="list-style-type: none"> • Select a wallpaper from the built-in options or upload a photo. • Click Apply to save all changes. |
| 3 | 2-step Verification | Click Get Started to open the configuration wizard. For details, see Enabling 2-step Verification . |
| 4 | Change Password | <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 QTS: When enabled, QTS prompts users for confirmation whenever they try to leave the desktop (by clicking the Back button or closing the browser). QNAP recommends enabling this setting. • Reopen windows when logging back into NAS: When enabled, the current desktop settings (including all open windows) are retained until the next session. • Show the desktop switching button: When enabled, QTS displays the desktop switching buttons < > on the left and right sides of the desktop. • Show the link bar on the desktop: When enabled, QTS displays the link bar on the bottom of the desktop. • Show the Dashboard button: When enabled, QTS displays the button to show the dashboard on the taskbar. • Show the NAS time on the desktop: When enabled, QTS displays the current NAS time, day, and date at the bottom-right of the desktop. • Keep Main Menu open after selection: When enabled, QTS keeps the main menu pinned to the desktop after you open it. • Show a list of actions when external storage devices are detected: When enabled, QTS displays an Autoplay dialog box whenever an external storage device is inserted into a USB or SATA port. • Click Apply to save all changes. |

Dashboard





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



Tip

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


| No. | Section | Displayed Information | User Actions |
|-----|----------------------|---|---|
| 1 | System Health | <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 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 > Storage . |
| 6 | Storage | For each volume: <ul style="list-style-type: none"> • Status • Used space • Available space • Folder size For each storage pool: <ul style="list-style-type: none"> • Status • Used space • Available space • Volume size | <ul style="list-style-type: none"> • Click the heading to open the Storage Resource screen in the Resource Monitor window. • Click  to switch between volume and storage pool information. |
| 7 | Online Users | <ul style="list-style-type: none"> • Username • Session duration • IP address | Click the heading to open Control Panel > System > QuLog Center > Online Users . |

| No. | Section | Displayed Information | User Actions |
|-----|-----------------|---|--|
| 8 | Scheduled Tasks | <ul style="list-style-type: none"> • Task type • Task summary • Task name • Timestamp • Status | Use the filters to view tasks that were executed within a specific period. |
| 9 | News | Links to QNAP announcements | Click the heading to open the relevant pages on the QNAP website. |





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.</p> <p>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 <p> Note This menu item only appears on models with certain hardware specifications.</p> | <ul style="list-style-type: none"> • Open a system utility or application in the QTS 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.</p> <p>The following are the default applications:</p> <ul style="list-style-type: none"> • Hybrid Backup Sync 3 • File Station • Helpdesk • License Center • Multimedia Console • Notification Center • QTS SSL Certificate | |

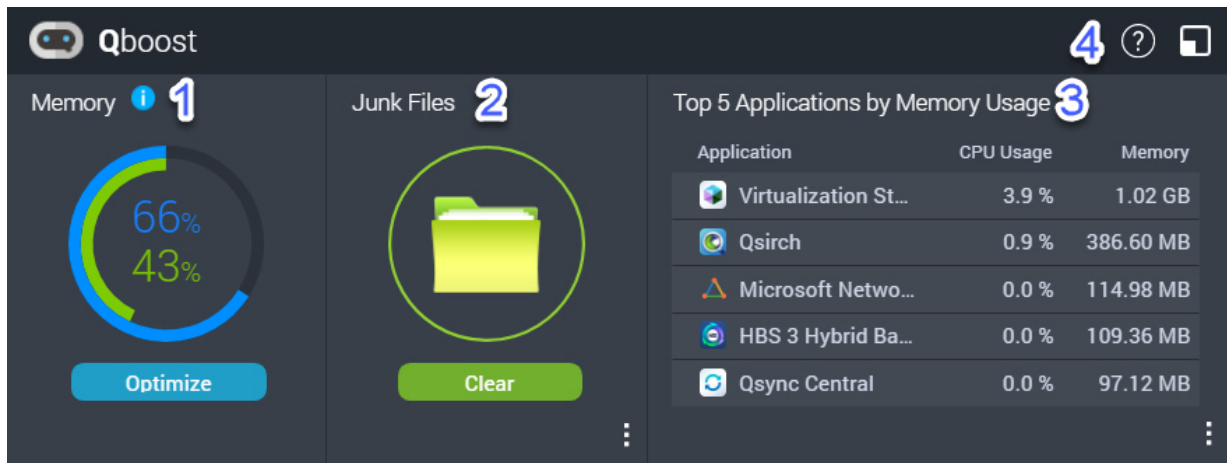
Desktop





| # | Element | Description | Possible User Actions |
|---|----------------|--|--|
| 1 | Wallpaper | This is a digital image that is used as a background for the QTS desktop. Users can either select from one of the provided wallpapers or upload an image | Change the wallpaper in the Options window. |
| 2 | Shortcut icons | Each icon opens an app or a utility. When you install an application, QTS automatically creates a desktop shortcut. The following are the default shortcuts: <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 | This notifies the user about important system events that may or may not require user action. Notifications appear in the lower right corner of the desktop. | Click the notification to open the corresponding utility or app. |

Qboost



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

| # | Section | Description | User Actions |
|---|------------------------------------|---|--|
| 1 | Memory | <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).</p> <p>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> <p> Warning Setting a schedule may force an application to stop in the middle of a task.</p> | <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 |
| Delete a schedule. | Click  to delete the schedule and disable an application or service. |
| Remove an application. | Click  . This function applies only to applications that are available in App Center. |

Getting Started

1. Log in to the NAS as an administrator.
The default administrator account is `admin`.
For details, see [NAS Access](#).
2. Plan how you want to combine or divide the available storage space.
For details, see [Volume Configuration](#).
3. Optional: Create one or more storage pools.
You must create at least one storage pool in order to create multiple volumes.
For details, see [Creating a Storage Pool](#).
4. Create one or more volumes.
You must create at least one volume in order to store files on the NAS.
For details, see [Volume Creation](#).
5. Create user accounts.
QNAP recommends creating a user account for each person that requires access to the NAS.
For details, see [Creating a Local User](#).
6. Optional: Create user groups.

User groups help you to easily manage user accounts.
For details, see [Creating a User Group](#).

- 7.** Optional: Create shared folders.
QTS creates four default shared folders.
For details, see [Shared Folders](#).
- 8.** Edit shared folder permissions.
Permissions enable you to control who can view and modify files in a shared folder.
For details, see [Shared Folder Permissions](#).
- 9.** Map the shared folders as network drives on your computer.
For details, see [Shared Folder Access](#).
- 10.** Store and manage files.
For details, see [File Station](#).


2. System Settings



General Settings

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

Configuring System Administration Settings

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

| Field | User Action |
|--------------------|--|
| Server name | <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. • The host name must contain one or more letters. • The host name cannot consist of numbers only. • The host name cannot start with a dash. |
| 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"> Specify a port number. Optional: Select Force secure connection (HTTPS) only to require all users to connect to the NAS using only HTTPS. |
| Custom "Server" HTTP header | Select this option to specify a server HTTP header. |
| Do not allow QTS embedding in IFrames | <ol style="list-style-type: none"> Select this option to prevent websites from embedding QTS using IFrames. Click Allowed Websites to allow a specific website to embed QTS 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. |
| Enable X-Content-Type-Options HTTP header | Select this option to protect your device from attacks that exploit MIME sniffing vulnerabilities. |

3. Click **Apply**.

Configuring Time Settings



Important

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

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

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

| Option | User Action |
|---|---|
| Manual setting | Specify the date and time. |
| Synchronize with an Internet time server automatically | <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 |
| 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. |

| Action | Steps |
|-----------------|--|
| Edit DST data | <ol style="list-style-type: none"> Select a DST schedule from the table. Click . Specify a time period and the number of minutes to offset. Click Apply. |
| Delete DST data | <ol style="list-style-type: none"> Select a DST schedule from the table. Click Delete. 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.

- Go to **Control Panel > System > General Settings > Codepage**.
- Select the language of your operating system.
- 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.

- Go to **Control Panel > System > General Settings > Region**.
- 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

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

| Field | User Action |
|------------------------------|---|
| Login screen template | Select a template for the login screen. |

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

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

4. Click **Apply**.

Enabling or Disabling Console Management

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

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



Note

Enable Console Management is enabled by default.

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

Security

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 . |

| Option | Description | User Action |
|-------------------|--|--|
| Use IP deny list | The NAS cannot connect to any IP address or network domains included in the IP deny list. | <p>a. Select Deny connections from the list.</p> <p>b. Click Add. The IP configuration window appears.</p> <p>c. Specify an IP address, netmask, or IP range.</p> <p>d. Click Create.</p> <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. | <p>a. Select Allow connections from the list only.</p> <p>b. Click Add. The IP configuration window appears.</p> <p>c. Specify an IP address, netmask, or IP range.</p> <p>d. Click Create.</p> <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 an SSL certificate from a trusted provider.

Replacing the SSL Certificate and Private Key



Warning


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

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

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

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

| Option | User Action |
|--------------------|--|
| Import certificate | <ol style="list-style-type: none"> a. Click Browse to upload a valid certificate and private key. b. Optional: Click Browse to upload an intermediate certificate. |

| Option | User Action |
|--------------------------------|---|
| 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. Specify a valid email address. c. Optional: Specify an alternative name. <div style="border-left: 2px solid orange; 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 |

6. Click **Apply**.

Downloading the SSL Certificate and Private Key

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

Restoring the Default SSL Certificate and Private Key

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

Configuring the Password Policy



Important

The following password policy is configured by default:

- English letters: No restrictions

- Digits: Enabled
- Minimum length: 8

1. Go to **Control Panel > System > Security > Password Policy** .
2. Optional: Under **Password Strength**, configure any of the following password criteria.

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

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



Important

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

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



Hardware

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

Configuring General Hardware Settings

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


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

| 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. |
| Enable light signal alert | Select this option to allow the status LED to flash when free space on the NAS is less than the set value. |
| Enable write cache (EXT4 delay allocation) | <p>If the NAS disk volume uses EXT4, select this option for higher write performance.</p> <p>If the NAS is set as a shared storage in a virtualized or clustered environment, disable this option.</p> <p> Warning When this option is enabled, an unexpected system shutdown may lead to data loss.</p> |
| 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 | <p>Select this option to turn on the LED, set its brightness level, and set a schedule for brightness setting.</p> <p> Note This function is only applicable for some models.</p> |

3. Click **Apply**.

Configuring Audio Alert Settings

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

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

3. Click **Apply**.

Configuring Smart Fan Settings

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

**Note**

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

| Setting | User Action |
|---|--|
| Automatically adjust fan speed (recommended) | <p>Select from the two automatic fan speed adjustment options.</p> <ol style="list-style-type: none"> QTS monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. QTS adjusts the fan speed according to user-specified temperatures. <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. |
| Manually set fan speed | Move the slider to set the fan speed. |

- Click **Apply**.

Configuring Hardware Resource Settings

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

For details, see [Viewing Single Root I/O Virtualization \(SR-IOV\) Settings](#)

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

**Note**

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

| OS or Application | Description |
|-------------------|--|
| QTS | <p>QTS applications share expansion card resources for transcoding.</p> <ul style="list-style-type: none"> Select Hardware Transcoding to allow QTS software to use expansion card resources to speed up transcoding tasks. Only one card can be assigned to hardware transcoding. Select Output to use expansion card resources for video output of HD Station or Linux Station. Only one card can be assigned to output. |

| OS or Application | Description |
|------------------------|---|
| Virtualization Station | Virtualization Station has exclusive use of all expansion card resources. |
| Container Station | Container Station has exclusive use of all expansion card resources. |

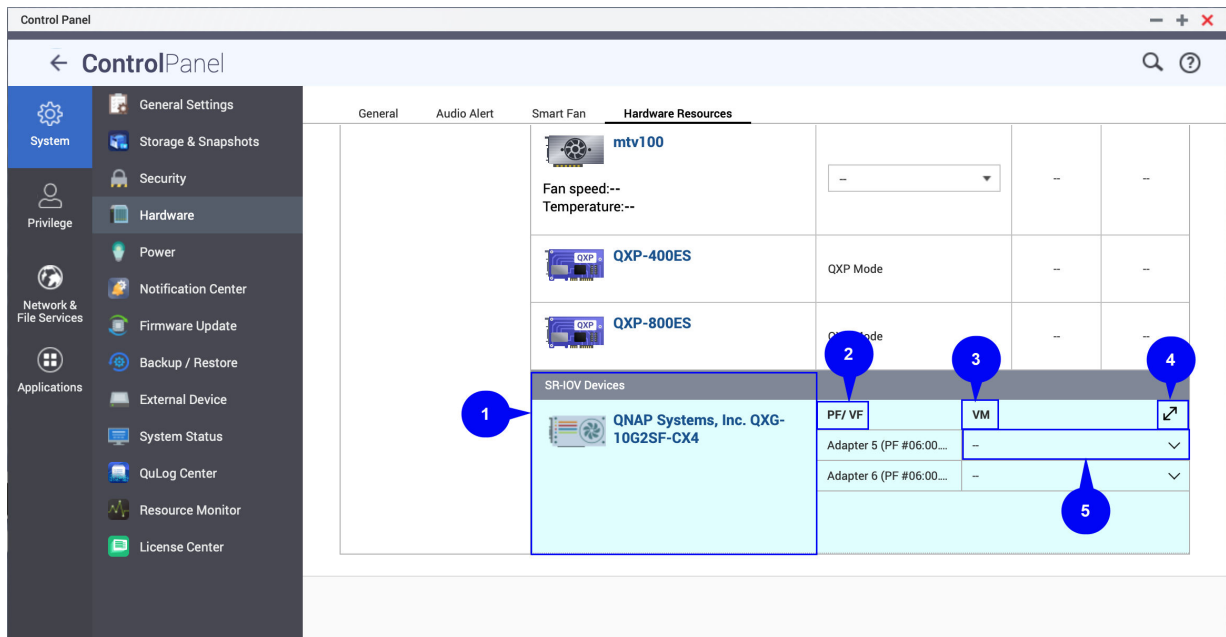
4. Click **Apply**.


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


You can view all Single Root I/O Virtualization (SR-IOV) devices mapped to your virtual machines on the **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 | SR-IOV Devices | Lists all the SR-IOV devices that are mapped to your virtual machine (VM). |
| 2 | PF/VF | Displays the physical function (PF) or virtual function (VF) configured to the SR-IOV device. |
| 3 | VM | Shows the virtual machines that are mapped to the PF or VF. |
| 4 | Resize | Click  to enlarge or minimize the SR-IOV device panel window. |

| No. | Settings | Description |
|-----|--------------|--|
| 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 Wake-on-LAN (WOL), select a NAS behavior after power outage, and specify power schedules.

EuP Mode

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

Configuring EuP Mode

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

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

3. Click **Apply**.

Wake-on-LAN (WOL)

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



Important

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

Enabling or Disabling Wake-on-LAN (WOL)

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

Power Recovery

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

Configuring the Power Recovery Settings

1. Go to **Control Panel > System > Power > Power Recovery** .


2. Select a power recovery setting.
 - Restore the previous NAS power state.
 - Turn on the NAS automatically.
 - Keep the NAS turned off.
3. Click **Apply**.

Power Schedule

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

Configuring the Power Schedule

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

| Task | User Action |
|---------------------------|---|
| Add a scheduled action |  Note One schedule is shown by default. <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. |
| Remove a scheduled action | <ol style="list-style-type: none"> a. Select one or multiple schedules. b. Click Remove. |

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

Firmware Update

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



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

| Update Method | Description |
|--------------------------|--|
| Using Live Update | Firmware updates are automatically detected by QTS and installed onto your device. For details, see Checking for Live Updates . |

| Update Method | Description |
|----------------------------|--|
| 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 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 <p> Important A computer is required for updating the firmware manually or through Qfinder Pro.</p> <ul style="list-style-type: none"> Ethernet cables <p> Important QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection is reliable during firmware updates.</p> |
| System reboot | QNAP recommends rebooting the NAS system before the firmware backup. |
| Administrator privileges | You must be a NAS administrator or have admin privileges to update firmware. |
| Stop NAS operations | QNAP recommends stopping all other NAS operations before the firmware update. The NAS must 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: |
| 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**.
QTS checks for available firmware updates. You can choose to update QTS if there is an available update.
3. Specify the auto update frequency.
4. Click **Apply**.
5. Optional: Select one or more of the following options.
 - Automatically check if a newer version is available when logging into the NAS web administration interface.
 - Join the QTS Beta program to receive beta update notifications.



Note

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

6. Click **Apply**.

Updating the Firmware Manually



Warning

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



Important

- Make sure you read through the [Firmware Update Requirements](#) before updating the firmware.
- The update may require several minutes or longer, depending on your hardware configuration and network connection.

1. Download the NAS firmware.
 - a. Go to <http://www.qnap.com/download>.
 - b. Select the number of drive bays on your NAS model.
 - c. Select your NAS model.
 - d. Read the release notes and confirm the following:
 - The NAS model matches the firmware version.
 - Updating the firmware is necessary.
 - Check for any additional firmware update setup instructions.

- e. Ensure that the product model and firmware are correct.
 - f. Select the download server based on your location.
 - g. Download the firmware package.
 - h. Click **Browse**.
 - i. Select a folder.
 - j. Save the downloaded firmware package.
 - k. Extract the firmware package file.
2. Go to **Control Panel > System > Firmware Update > Update System** .
 3. Click **Browse** and then select the extracted firmware package file.
 4. Click **Update System**.
A confirmation message window appears.
 5. Click **OK**.
The device is immediately restarted.



Note

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

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.
- QTS automatically downloads the available stable version firmware during the specified update time.

Updating the Firmware Using Qfinder Pro**Warning**

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

**Important**

- Make sure you read through the [Firmware Update Requirements](#) before updating QTS.
- The update may require several minutes or longer, depending on your hardware configuration and network connection. Do not power off the NAS during the update.

1. Download the NAS firmware.
 - a. Go to <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 QTS username and password.
Qfinder Pro displays the **Update Firmware** screen.

6. Select one of the following firmware update methods:

| Methods | Steps |
|-------------------------------|---|
| Update firmware manually | <ol 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 | <ol 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

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

Backing Up System Settings

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

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

Restoring System Settings



Warning

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

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


System Reset and Restore to Factory Default



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



Important

QNAP recommends backing up your data before performing this task.

| Option | Description | Steps |
|--------------------|--|---|
| Basic system reset | <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 QTS 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 QTS: <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. |
| Restore factory default settings and format all volumes | <p>This restores the default system settings and formats all disk volumes.</p> | <ol style="list-style-type: none"> 1. Go to Control Panel > System > Backup/Restore > Restore to Factory Default . 2. Click Restore Factory Defaults & Format All Volumes. <p> Important Selecting Restore Factory Defaults & Format All Volumes will delete all data on the NAS. To retain all files and data on the hard drive, see Reset to default settings.</p> <ol style="list-style-type: none"> 3. Choose to restart or shut down the NAS after the system is reset. 4. Click OK. |
| Reset to default settings | <p>This restores the default system settings without deleting the user data.</p> | <ol style="list-style-type: none"> 1. Go to Control Panel > System > Backup/Restore > Restore to Factory Default . 2. Click Reset Settings. |

| Option | Description | Steps |
|----------------------|--|--|
| Reinitialize the NAS | This deletes all data on the disks and reinstalls QTS. | <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. |

Restoring the Settings of a Default Shared Folder

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



Important

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

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

Restoring the Settings of a Non-Default Shared Folder

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



Important

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

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

External Device

USB Printer

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

Configuring USB Printer Settings


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



Warning

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

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

| Task | Action |
|----------------------------|--|
| View printer information | Click Printer Info . This displays the details of the selected printer. |
| View printer log | Click Printer Log . This displays the current and completed print jobs on the selected printer.  Tip You can stop, resume, or cancel ongoing or pending print jobs. You can also delete completed or pending print jobs. Click Clear to clear the history. |
| Clean up spool space | Click Clean Up Spool Space . This deletes the data stored in the printer spool. |
| Configure printer settings | Click Settings . This enables you to configure the following settings: <ul style="list-style-type: none"> • Stop printer sharing and clear print spool: Select this option to disable printing and delete all stored data on the selected printer. • Bonjour printer support: Select this option to introduce the printing service to the macOS users on your network. |

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

Creating a USB Printer Access List

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

1. Go to **Control Panel > System > External Device > USB Printer** .
QTS displays the detected USB printers on your network.

2. Specify access rights.
 - a. Beside **Access right**, select **Allow printing** or **Deny printing**.
 - b. Specify the IP addresses or domain names that you want to allow or deny.

**Tip**

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

3. Click **Apply**.

Uninterruptible Power Supply (UPS)

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



NAS Behavior During a Power Outage

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

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

Configuring the UPS Settings


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

| Mode | User Actions |
|-------------------|--|
| USB connection | <ol style="list-style-type: none"> Connect the UPS to the NAS using a USB cable. Select USB connection. Choose one of the following options. <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> <ol style="list-style-type: none"> (Optional) Select Enable network UPS master and then specify the IP addresses to which QTS sends notifications in the event of power failure. <p> Note This option can only be selected when the UPS is connected to the NAS via USB.</p> |
| SNMP connection | <ol style="list-style-type: none"> Connect the UPS to the same network as the NAS. Select SNMP connection. Specify the IP address of the UPS. Configure the SNMP community. Choose one of the following options. <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 UPS slave | <ol style="list-style-type: none"> Connect the UPS to the same network as the NAS. Select Network UPS slave. Specify the IP address of the UPS server. Choose one of the following options. <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, server name, model name, CPU, Intel QuickAssist Technology (Intel QAT) support, serial number, BIOS version, memory, firmware version, system up time, time zone, and filename encoding.</p> <p> Note Intel QuickAssist Technology support only appears when it is detected by QTS.</p> |
| Network Status | This screen displays the current network settings of each network interface. |
| System Service | This screen displays the current status of system services, such as antivirus, networking services, DDNS services, domain controllers, multimedia management, data backup management, surveillance management, remote servers, and VPN servers. |
| Hardware Information | This screen displays NAS hardware information, such as CPU usage, memory, disk temperature, power supply unit (PSU) status, and system fan speed. |

Resource Monitor

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

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

| Section | Description |
|-------------------------|---|
| Overview | This screen provides a general summary of CPU usage, memory usage, network usage, and ongoing processes on the NAS. |
| System Resource | <p>This screen uses line charts to display CPU usage, memory usage, network usage, and graphics card usage (if supported and installed) over time.</p> <p>You can hover the mouse pointer over a line chart to view the hardware usage at a specific time point.</p> <p> Tip 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.</p> <p>You can hover the mouse pointer over a line chart to view the storage activity at a specific point in time.</p> |

| Section | Description |
|------------------|---|
| 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 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, and show or hide columns.</p> |

3. Privilege Settings

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

Users

Default Administrator Account

The admin user account is the default administrator account. It can configure settings, create users, and install applications. You cannot delete this account. To prevent malicious actors from compromising your system due to easy passwords, QNAP strongly recommends changing the default admin password or creating another administrator account and disabling the default admin account. A new administrator account can perform the same actions as the default administrator account. There are two reasons for not disabling the default admin account. If you want to access the QNAP turbo NAS via Secure Shell (SSH) or Telnet, do not disable the default admin account. Also, if you're going to access Console Management, do not disable the default admin account.


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 QTS. <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) | <p>Specify an email address that will receive notifications from QTS. 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> |
| Send a notification mail to the newly created user (optional) | <p>When selected, QTS sends a message that contains the following information to the specified email address:</p> <ul style="list-style-type: none"> • URLs for connecting to the NAS <p> Tip You can edit the notification message.</p> |

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 a local user.
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. |
| Phone number (optional) | Specify a phone number that will receive SMS notifications from QTS. <div style="border-left: 2px solid #0070C0; padding-left: 10px; 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) | <p>Specify an email address that will receive notifications from QTS. 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> |
| Send a notification mail to the newly created user (optional) | <p>When selected, QTS sends a message that contains the following information to the specified email address:</p> <ul style="list-style-type: none"> • URLs for connecting to the NAS <p> Tip You can edit the notification message.</p> |

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

**Tip**

QNAP recommends denying access to applications and network services that the user does not require. Users without privileges to specific applications will not see it on their main menu.

7. Optional: Set a quota for the user.

**Note**

This option is only available when quotas are enabled.

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

**Note**

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

8. Click **Create**.

Creating Multiple Users

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

| Field | Description |
|---------------------------|--|
| User Name Prefix | Specify a username that contains a maximum of 23 ASCII characters and that does not: <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: <code>1</code> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p>Note QTS removes leading zeros in starting numbers. For example, <code>001</code> becomes <code>1</code>.</p> </div> |
| Number of Users | Specify the number of users (1–4095). Example: <code>5</code> |
| Password | Specify a password that contains a maximum of 64 ASCII characters. |



Note

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

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

| Field | Description |
|---------------------------|---|
| Hide network drive | Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder. |

| Field | Description |
|----------------------------|--|
| Lock File (Oplocks) | Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files. |
| Disk Volume | Select the data volume where the private network share will be created. |

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

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

User Account Lists

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

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

Creating a TXT User File

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



Important

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



Note

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

- Specify information for only one user on each line.

Example:

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

- Save the list as a TXT file.



Important

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

Creating a CSV User File

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, QTS 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, QTS overwrites existing user accounts that have duplicates on the imported user account list. |

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




Important

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

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

6. Click **Next**.

| File Type | User Action |
|------------|--|
| TXT or CSV | <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**.
QTS imports the user account list.

8. Click **Finish**.

Exporting Users

1. Go to **Control Panel > Privilege > Users** .
2. Click **Create > Import/Export Users** .
The **Import/Export Users** window appears.
3. Select **Export user and user group settings**.
4. Click **Next**.
QTS exports the user account list to your computer as a BIN file.











Tip

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

Modifying User Account Information

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

| Task | User Action |
|----------------------------|---|
| Change password | <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. |
| Edit account profile | <ol style="list-style-type: none"> a. Under Action, click  . The Edit Account Profile window appears. b. Edit the settings. The Edit Account Profile window provides the following settings not included in the Create a User window: <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, QTS prevents the user from changing the password. • Disable this account: Select this option to disable the user account. You can either select to disable the account Now or specify an Expiry Date. c. Modify the quota for the user. <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> <ol style="list-style-type: none"> d. Click OK. |
| Edit user group membership | <ol style="list-style-type: none"> a. Under Action, click  . The Edit User's Groups window appears. b. Select or deselect user groups. c. Click Apply. |

| Task | User Action |
|--------------------------------|---|
| Edit shared folder permissions | <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. Optional: Select **Also delete the selected user(s)' home folders and data**.
5. Click **Yes**.

Home Folders

Enabling home folders creates a personal folder for each local and domain user on the NAS. When a home folder is created, the user's home folder appears as a shared folder called `home`. Users can access their home folder through Microsoft networking, FTP, and File Station.

All user home folders are located in the `homes` shared folder. By default, only 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 volume.
Home folders are stored on the selected volume.
5. Click **Apply**.

User Groups

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

Default User Groups

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

Creating a User Group

1. Go to **Control Panel > Privilege > User Groups**.
2. Click **Create**.
The **Create a User Group** window appears.
3. Specify the **User group name**.
The user group name can contain 1 to 128 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Multi-byte characters: Chinese, Japanese, Korean, and Russian
 - Dashes (-)
4. Optional: Specify a description that contains a 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 | <p>a. Under Action, click . The View Group Details window appears.</p> <p>b. Modify the description.</p> <p>c. Modify the quota.</p> <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> <p>d. Click OK.</p> |
| Edit user group members | <p>a. Under Action, click . The Edit User Group window appears.</p> <p>b. Select or deselect users.</p> <p>c. Click Apply.</p> |
| Edit shared folder permissions | <p>a. Under Action, click . The Edit Shared Folder Permissions window appears.</p> <p>b. Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions.</p> <p>c. Click Apply.</p> <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

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



Important

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

| Folder | Description |
|------------|---|
| Download | This is the default folder for Download Station. The folder stores content downloaded in QTS. 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 . |
| Public | This folder can be used by any user account. The default permission of this folder is Read Only. For details, see Shared Folder Permissions . |
| Web | This folder stores content from the Web Server utility, which you can manage in Control Panel > Applications > Web Server . <div data-bbox="587 1111 644 1169" data-label="Image"> </div> <div data-bbox="667 1104 738 1135" data-label="Section-Header"> <h4>Note</h4> </div> <div data-bbox="667 1135 1308 1200" data-label="Text"> <p>You must enable Web Server automatically to create this default shared folder.</p> </div> |

Restoring Default Shared Folders


You can restore default shared folders that were deleted.

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

QTS restores the default shared folders.

Creating a Shared Folder

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

| Field | Description |
|---------------------------|---|
| Folder Name | Specify a folder name that contains 1 to 64 characters and that does not: <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 QTS. |
| Disk Volume | Specify the volume on which the shared folder will be created. |
| Qtier Auto Tiering | When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier . This setting is only available if you select a Qtier-enabled storage pool. <div style="border-left: 2px solid orange; padding-left: 10px; margin-top: 10px;">  Tip You can also enable auto-tiering from the Shared Folders screen. </div> |
| Path | <ul style="list-style-type: none"> • Specify path automatically: Creates a new root folder on the selected volume using the specified shared folder name. • Enter path manually: Select an existing folder as the root folder. |


4. Optional: Configure user access permissions.

- a. Under **Configure access privileges for users**, click **Edit**.
- b. Specify the access permissions for users.
For details, see [Shared Folder Permissions](#).


5. Optional: Enable folder encryption.


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

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

| Field/Option | Description |
|----------------------------|---|
| Save encryption key | <p>When enabled, QTS automatically unlocks the shared folder after the NAS restarts.</p> <p>When disabled, the administrator must unlock the folder after the NAS restarts.</p> <p>For details, see Unlocking a Shared Folder.</p> <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> |

6. 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. 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 blue; padding-left: 10px; margin-top: 10px;">  <p>Note 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. |
| Enable access-based share enumeration (ABSE) | When enabled, users can only see the shared folders that they have permission to mount and access. Guest account users must enter a username and password to view shared folders. |
| Enable access-based enumeration (ABE) | When enabled, users can only see the files and folders that they have permission to access. |

| Option | Description |
|--|---|
| Set this folder as the Time Machine backup folder (macOS) | <p>When enabled, the shared folder becomes the destination folder for Time Machine in macOS.</p> <p> Important</p> <ul style="list-style-type: none"> • If space in the folder is insufficient when starting a new Time Machine backup, QTS automatically deletes the oldest Time Machine backup in the folder to free up space. • You should disable Enable Network Recycle Bin when Set this folder as the Time Machine backup folder (macOS) is selected to prevent automatically deleted Time Machine backups from filling the recycle bin. |


7. Click **Create**.



Tip

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

Editing Shared Folder Properties



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





Important

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

| Setting | Description |
|---------------------------|--|
| Folder Name | <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) | <p>Specify a comment that contains 1 to 128 ASCII characters. The information is for your reference and is not used by QTS.</p> |
| Disk Volume | <p>Specify the volume on which the shared folder will be created.</p> |

| Setting | Description |
|---|--|
| Qtier Auto Tiering | <p>When enabled, Qtier performs auto-tiering on data in the folder. For details, see Qtier. This setting is only available if you select a Qtier-enabled storage pool.</p> <p> Tip You can also enable auto-tiering from the Shared Folders screen.</p> |
| Path | Modify the folder path. |
| Hide network drive | Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder. |
| Lock File (Oplocks) | Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files. |
| SMB Encryption | This option is available only when SMB3 is enabled. 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 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. |

| Setting | Description |
|--|---|
| Encrypt this folder | <p>Folder encryption protects folder content against unauthorized data access when the drives are physically stolen. Specify the following information.</p> <p>a. Input Password Specify a password that contains 8 to 32 characters except the following: " \$: = \ This field does not support multibyte characters.</p> <p>b. Verify Password The password must match the previously specified password.</p> <p>c. Save encryption key When enabled, QTS automatically unlocks the shared folder after the NAS restarts. When disabled, the administrator must unlock the folder after the NAS restarts. For details, see Unlocking a Shared Folder.</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. |
| 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> <p> Important</p> <ul style="list-style-type: none"> • If space in the folder is insufficient when starting a new Time Machine backup, QTS automatically deletes the oldest Time Machine backup in the folder to free up space. • You should disable Enable Network Recycle Bin when Set this folder as the Time Machine backup folder (macOS) is selected to prevent automatically deleted Time Machine backups from filling the recycle bin. |
| Migrate to Snapshot Shared Folder | Migrate the shared folder to a snapshot shared folder. For details, see Migrating to a Snapshot Shared Folder . |

5. Click **OK**.

Refreshing a Shared Folder

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

Removing Shared Folders

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



Note

Default shared folders cannot be removed.

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

Enabling Daily Updates for Shared Folders

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

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

Snapshot Shared Folders

A snapshot shared folder is a shared folder created on a dedicated volume and allows users to quickly recover data by restoring a folder or reverting a volume from a snapshot. Users can also set folder quotas for snapshot shared folders.


For details on snapshots, see [Storage & Snapshots](#).

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

Creating a Snapshot Shared Folder

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

3. Specify the following information:

| Field | Description |
|------------------------------|---|
| Folder Name | Specify a folder name that contains 1 to 64 characters and that does not: <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. |
| Storage Pool | Specify the storage pool where the shared folder will be created. |
| Space Allocation | Select one of the following space allocation options: <ul style="list-style-type: none"> • Thick provisioning • Thin provisioning |
| Qtier Auto Tiering | When enabled, Qtier performs auto-tiering on data in the folder. This setting is only available if you select a Qtier-enabled storage pool. <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>Tip You can also enable auto-tiering from the Shared Folders screen.</p> </div> </div> |
| Allocate folder quota | You can allocate a folder quota for the snapshot shared folder. |

4. Optional: Configure user access permissions.

a. Under **Configure access privileges for users**, click **Edit**.

b. Specify the access permissions for users.
For details, see [Shared Folder Permissions](#).

5. Optional: Configure advanced settings.

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

6. Click **Create**.**Migrating to a Snapshot Shared Folder**

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

2. Select the folder you want to migrate to a snapshot shared folder.

3. Click **Migrate to Snapshot Shared Folder**.

The **Migrating shared folder to a snapshot shared folder** wizard appears.





4. Select the location for the snapshot shared folder.

5. Click **Next**.


6. Optional: Free up storage pool space on the volume.


**Note**

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

| Option | User Action |
|---|---|
| Release unused guaranteed snapshot space | <p> Note This option is only available if guaranteed snapshot space has been allocated to the storage pool.</p> <ol style="list-style-type: none"> Click Set up now. The Snapshot Settings window appears. Configure the snapshot settings to release space. For details, see Storage & Snapshots. Click OK. |
| Run a space reclaim to release used space on thin volumes | <p> Note This option is only available if the storage pool contains a thin volume with reclaimable space.</p> <ol style="list-style-type: none"> Click Run now. A dialog box appears. Click OK to reclaim the available storage space. QTS reclaims the used space. A dialog box appears. Click OK. |
| Convert a thick volume to a thin volume to release unallocated space | <p> Note This option is only available if the storage pool contains a thick volume.</p> <ol style="list-style-type: none"> Select a volume to convert. Click Run now. The Convert to Thin Volume window appears. <p> Warning Converting a volume deletes all existing snapshots on the volume.</p> <ol style="list-style-type: none"> Click Apply. QTS converts the volume. |

7. Configure the snapshot shared folder.

| Field | Description |
|---------------------------|--|
| Qtier Auto Tiering | <p>When enabled, Qtier performs auto-tiering on data in the folder. This setting is only available if you select a Qtier-enabled storage pool.</p> <p> Tip You can also enable auto-tiering from the Shared Folders screen.</p> |

| Field | Description |
|------------------------------|--|
| Space Allocation | Select one of the following space allocation options: <ul style="list-style-type: none"> • Thick provisioning • Thin provisioning |
| Allocated space quota | Specify a quota for the snapshot shared folder. <div style="display: flex; align-items: flex-start; margin-top: 10px;">  <div> <p>Tip</p> <p>Click Set to Max to allocate all remaining storage pool space to the volume.</p> </div> </div> |

8. Click **Next**.
9. Review the settings.
10. Click **OK**.

ISO Shared Folders

Users can mount ISO image files on the NAS as ISO shared folders and access them without having to burn discs. By default, most NAS models support up to 256 ISO shared folders.

ISO Shared Folder Requirements


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

| NAS Model | | |
|--|---|---|
| TS-1x: <ul style="list-style-type: none"> • TS-110 • TS-112 • TS-119 • TS-119P+ • TS-120 • TS-121 | TS-2x: <ul style="list-style-type: none"> • TS-210 • TS-212 • TS-219 • TS-219P • TS-219P+ • TS-220 • TS-221 | Other models: <ul style="list-style-type: none"> • TS-410 |

Mounting an ISO File as a Shared Folder

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

5. Specify the following information.

| Field | Description |
|----------------------|---|
| Folder Name | <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. | <ol style="list-style-type: none"> Click Next. Review the settings. |
| | By User | Selecting this option allows you to configure access permissions to the ISO shared folder at the user level. | <ol style="list-style-type: none"> Click Next. Configure the user account access rights for the ISO shared folder. Click Next. Review the settings. |
| | By User Group | Selecting this option allows you to configure access permissions to the ISO shared folder at the user group level. | <ol style="list-style-type: none"> Click Next. Configure the user group access rights for the ISO shared folder. Click Next. Review the settings. |

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

Shared Folder Permissions

| Permission | Description |
|-----------------|---|
| Read Only (RO) | The user or user group can read files in the shared folder, but not write them. |
| Read/Write (RW) | <p>The user or user group can read and write files in the shared folder.</p> <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> |
| 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. Under **Select permission type**, select a permission type to edit.
5. Perform any of the following tasks.


| Permission Type | Description | User Action |
|------------------------------------|---|---|
| Users and groups permission | Edit user and user group permissions for shared folders that can be accessed through Windows, macOS, FTP, and File Station. | <p>a. Specify permissions for each user and user group.</p> <p>b. Optional: Add a user to the list of users with permissions for the shared folder.</p> <ol style="list-style-type: none"> 1. Click Add. The Select users and groups window appears. 2. Select the type of user or user group from the drop-down menu in the upper left. 3. Specify the permissions for the users you want to add. 4. Click Add. QTS adds the users and their corresponding permissions to the list. <p>c. Optional: Remove a user from the list of users with permissions for the shared folder.</p> <ol style="list-style-type: none"> 1. Click the user you want to remove. 2. Click Remove. QTS removes the user from the list. <p>d. Optional: Modify guest access rights. Under Guest Access Right, select the permission type for guest accounts.</p> |
| NFS host access | Edit NFS host access rights for shared folders. | <p>a. Select Access right to enable NFS access rights.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <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> </div> <p>b. Under Host / IP / Network, enter an IP address or domain name.</p> <p>c. Optional: Add an NFS host. Under Allowed IP Address or Domain Name, click Add. QTS adds an entry to the list.</p> <p>d. Optional: Delete an NFS host.</p> <ol style="list-style-type: none"> 1. Select an NFS host from the list. 2. Click Delete. |

| Permission Type | Description | User Action |
|---|---|---|
| Microsoft Networking host access | Specify which computers can access shared folders through Microsoft Networking. | <ol style="list-style-type: none"> a. Add a Microsoft Networking host. <ol style="list-style-type: none"> 1. Click Add. QTS adds an entry to the list. 2. Under Host / IP / Network, enter an IP address or domain name. b. Optional: Delete a Microsoft Networking host. <ol style="list-style-type: none"> 1. Select a Microsoft Networking host from the list. 2. Click Delete. |

6. Click **Apply**.

Configuring Advanced Folder Permissions

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

| Option | Description |
|---|---|
| Enable Advanced Folder Permissions | <p>When enabled, users can assign folder and subfolder permissions to individual users and user groups.</p> <p> Note SMB/NFS mounted shared folders do not support advanced folder permissions.</p> |
| Enable Windows ACL support | When enabled, users can only configure folder and subfolder permissions from Windows File Explorer. |

3. Click **Apply**.

Conflicts in Shared Folder Permissions

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

1. No Access/Deny
2. Read/Write (RW)
3. Read Only (RO)

| User Permission | User Group Permission | Actual Permission |
|-----------------|-----------------------|-------------------|
| No Access | No Access | No Access |
| Read Only | | No Access |
| Read/Write | | No Access |
| Not Specified | | No Access |

| User Permission | User Group Permission | Actual Permission |
|-----------------|-----------------------|---|
| 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 |
| Not Specified | | <ul style="list-style-type: none"> • Shared folders through Samba/AFP: Read/Write • Shared folders through NFS: Read Only |
| 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 QTS folder tree file to avoid parsing errors.

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

Exporting Folder Trees



Note

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

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



Tip

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

4. Click **Finish**.

Shared Folder Encryption


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

Encrypting a Shared Folder



Note

- Default shared folders cannot be encrypted.
- The volume or path of an encrypted folder cannot be changed.
- Encrypted folders cannot be accessed through NFS.

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

| Field/Option | Description |
|----------------------------|---|
| Input Password | Specify a password that contains 8 to 32 characters except the following: " \$: = \ This field does not support multibyte characters. |
| Verify Password | The password must match the previously specified password. |
| Save encryption key | When enabled, QTS automatically unlocks the shared folder after the NAS restarts. When disabled, users must unlock the folder after restarting the NAS. For details, see Unlocking a Shared Folder . <div data-bbox="592 1464 651 1525" data-label="Image"> </div> Note QNAP strongly recommends exporting and saving the encryption key. For details, see Configuring Encryption Settings . |

The **Folder Encryption** window appears.

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

Configuring Encryption Settings

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



3.  Under **Action**, click . The **Encryption Management** window appears.



Note

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


4. Perform any of the following tasks.

| Task | User Action |
|----------------------------------|---|
| Download the encryption key file | <ol style="list-style-type: none"> Go to Download. Enter the encryption password. Click OK. QTS exports the encryption key file to your computer as a TXT. |
| Save the encryption key | <ol style="list-style-type: none"> Go to Save. Select Mount automatically on start up. When enabled, QTS automatically unlocks the shared folder after the NAS restarts. Enter the encryption password. Click OK. QTS saves the encryption key. |
| Lock the shared folder | <ol style="list-style-type: none"> Go to Lock. Optional: Select Forget the saved key. <ul style="list-style-type: none">  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. Click OK. QTS locks the folder. <ul style="list-style-type: none">  Note <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. |

Unlocking a Shared Folder

- Go to **Control Panel > Privilege > Shared Folders > Shared Folder** .
- 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, QTS automatically unlocks the shared folder after the NAS restarts. <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>Note This option is selected by default.</p> </div> </div> |
| Upload Encryption Key File | <ol style="list-style-type: none"> a. Click Browse. b. Select the encryption key file. |

5. Click **OK**.

Shared Folder Access

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

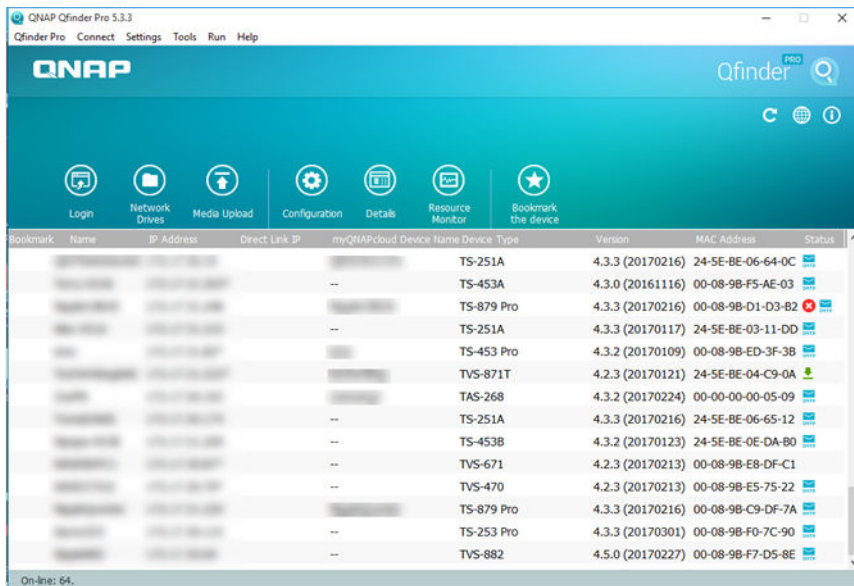
For Windows and Mac, you can use Qfinder Pro to map or mount your NAS shared folders. Qfinder Pro is a desktop utility that enables you to locate and access the QNAP NAS devices in your local area network.

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

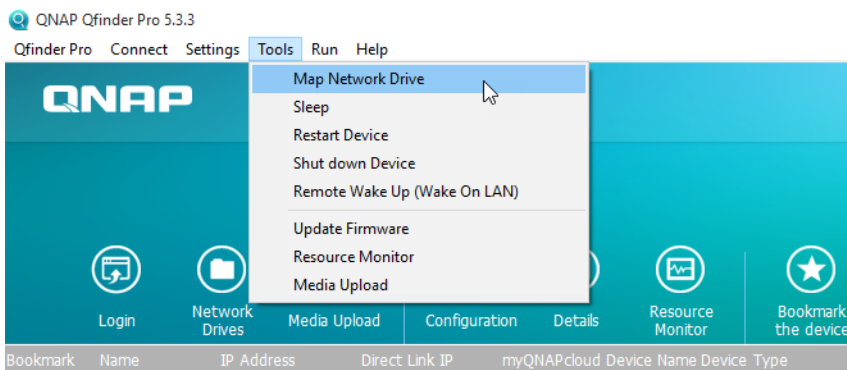
Mapping a Shared Folder on a Windows Computer

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

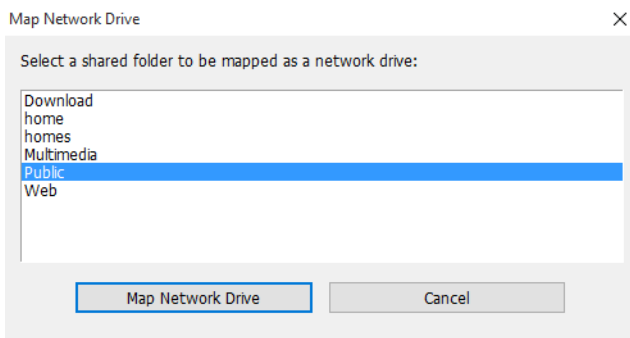
1. Power on the NAS.
2. Connect the NAS to your local area network.
3. Open **Qfinder Pro**.
Qfinder Pro displays all QNAP NAS devices in your local area network.



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

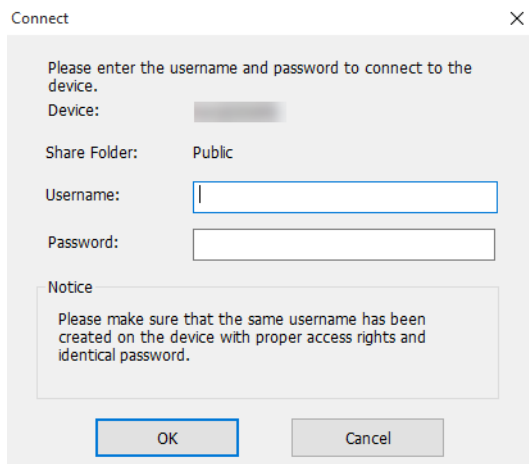


6. Select a shared folder.
7. Click **Map Network Drive**.

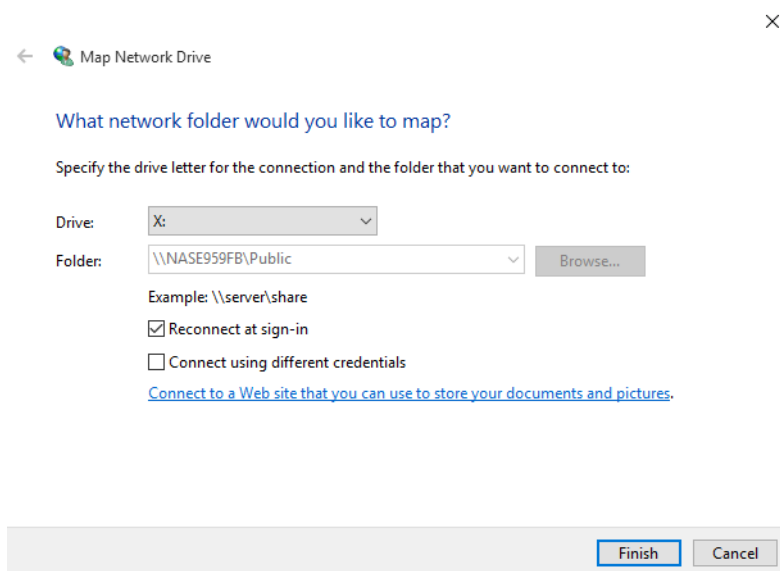


8. Specify your QTS username and password.

9. Click **OK**.



10. Specify the following information.



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

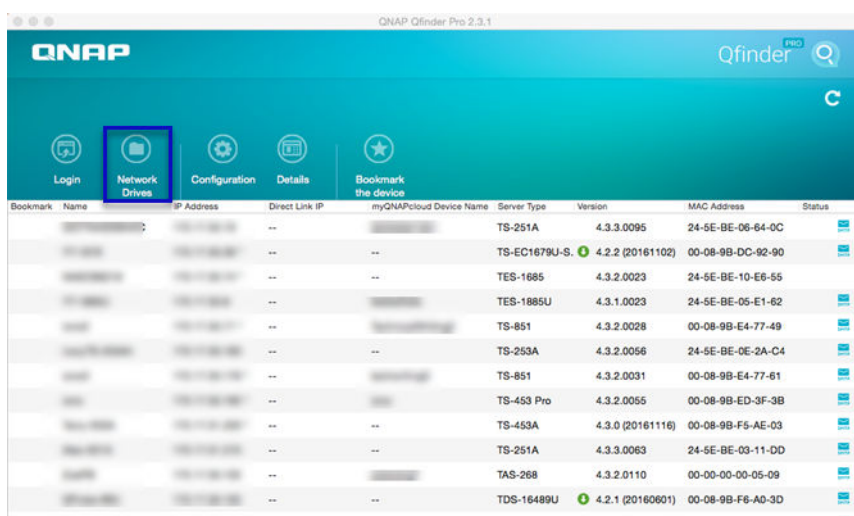
11. Click **Finish**.

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

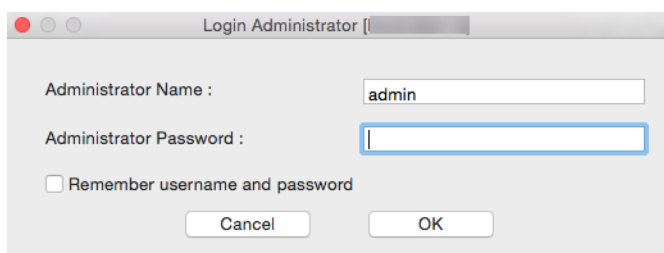
Mounting a Shared Folder on a Mac Computer

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

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

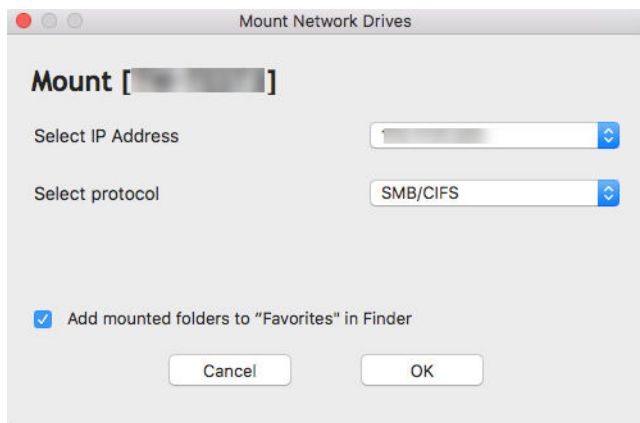


6. Specify your QTS username and password.
7. Click **OK**.



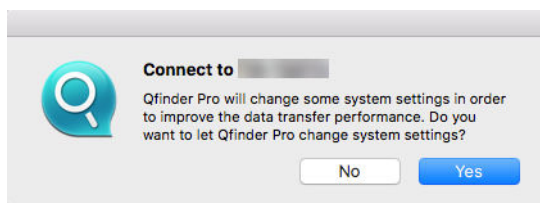
The **Mount Network Drives** window opens.

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

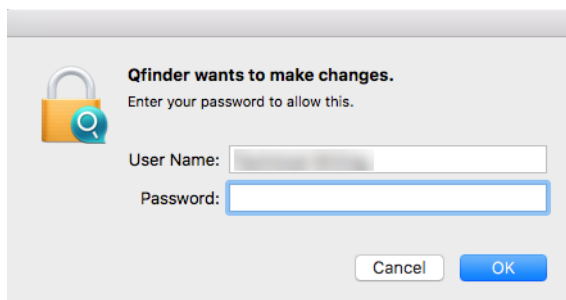


A confirmation message appears.

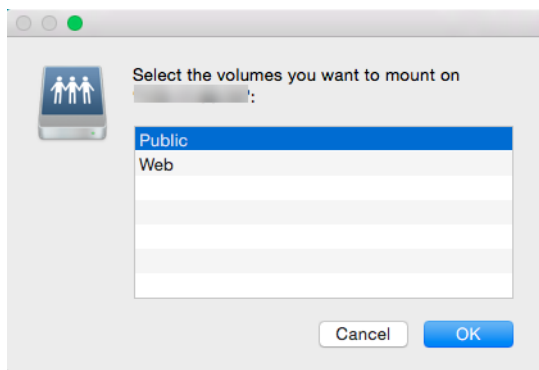
10. Click **Yes**.



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



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



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

Mounting a Shared Folder on a Linux Computer

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

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



Tip

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

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

3. Specify your NAS username and password.

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

Quota

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

QTS provides three types of quota settings.

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

**Note**

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

**Important**

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

**Tip**

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

Enabling Quotas

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

**Note**

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

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

Editing Quota Settings

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

**Tip**

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

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

**Important**

Individual quotas may override group quotas.

For details, see [Quota Conflicts](#).

6. Click **OK**.

Exporting Quota Settings

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

QTS exports the quota settings as a CSV file.

Quota Conflicts

QTS uses the following hierarchy to resolve quota conflicts.

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

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

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

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



Note

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

Domain Security

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

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



Note

QTS supports AD running on Windows Server 2008 R2, 2012, 2012 R2, 2016, 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.
QTS automatically generates the **NetBIOS domain name**.
6. Specify the IP address of the AD DNS server.
7. Optional: Select **Obtain DNS server address automatically by DHCP server**.
8. Click **Next**.
9. Select a domain controller.
10. Select the server signature rule for the domain.

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

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

Configuring AD Authentication Manually

Verify the following before starting this task:

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

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



Note

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

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



Note

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

5. Select the server signature rule for the domain.

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



- Click **Join**.

AD Server and Domain Names

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

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

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

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

Enabling Trusted Domain Authentication

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

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

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



Note

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

- Click **Apply**.
The **Advanced Options** window closes.
- 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

- Go to **Control Panel > Privilege > Domain Security**.
- Select **LDAP authentication**.
- Select the type of LDAP server.
- 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. ldaps:// (ldap + TLS): Use an encrypted connection with TLS. The default port is 389. Newer versions of LDAP servers normally use this port. ldaps:// (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 Type | Fields | User Action |
|-------------------------------|--|---|
| LDAP server of the remote NAS | IP address or NAS name | Specify the server IP address or the name of the NAS. |
| | LDAP domain | Specify the LDAP domain name. |
| | Password | Specify the NAS administrator password. |
| LDAP server of the local NAS | N/A | N/A |
| IBM Lotus Domino | This server type includes the same fields as Remote LDAP server , in addition to the following: | |
| | uidNumber | Specify the uid number. Select HASH . |
| | gidNumber | Specify the gid number. Select HASH . |

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

6. Select which users are allowed to access the NAS.



Note

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

7. Click **Finish**.

LDAP Authentication Options

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

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

| 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**.


QTS displays the list of domain users.

3. Locate a user.
4. Perform any of the following tasks.

| Task | User Action |
|--------------------------------|--|
| Edit an account profile | <p>a. Under Action, click . The Edit Account Profile window appears.</p> <p>b. Edit the user quota.</p> <p> Note User quotas must be enabled for this option to appear. For details, see Enabling Quotas.</p> |
| Edit shared folder permissions | <p>a. Under Action, click . The Edit Shared Folder Permission window appears.</p> <p>b. Edit the user's permissions for each shared folder. For details, see Shared Folder Permissions.</p> |
| 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**.
QTS displays the list of domain user groups.
3. Locate a user group.
4. Perform any of the following tasks.

| Task | User Action |
|--------------------|---|
| View group details | <p>Under Action, click . The View Group Details window appears. QTS displays the group name and group users.</p> |

| Task | User Action |
|--------------------------------|---|
| Edit shared folder permissions | <ol style="list-style-type: none"> a. Under Action, click . The Edit Shared Folder Permission window appears. b. Edit the user group's permissions for each shared folder. For details, see Shared Folder Permissions. |

**Tip**

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

5. Click **Apply**.

Domain Controller

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

Enabling a Domain Controller

**Important**

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

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

**Important**

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

3. Select the domain controller mode.

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

4. Specify the following information.

| Domain Controller Mode | Field | Description |
|--------------------------------|------------------------|--|
| Domain Controller | Domain | Specify the domain. |
| | Administrator Password | Specify an administrator password between 8 and 127 characters that contains at least one of each of the following: <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. |
| • Additional Domain Controller | Domain | Specify the domain. |
| | Domain DNS IP | Specify the domain DNS IP. |
| • 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: " + = / \ : * ? < > ; [] % ` ` ' |
| 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 QTS. For details, see Email Notifications . |


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

| Setting | Description |
|---|---|
| User must change the password at first logon | The user must change the password after logging in for the first time. |
| Account expiration | Set an expiration date for the account. <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 QTS 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**.
QTS creates the accounts and adds them to the list of domain users.
6. Click **Finish**.

Domain User Account Lists

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

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

Creating a TXT Domain User File

1. Create a new file in a text editor.
2. Specify domain user information in the following format.

```
Username,Password,Description,Email
```



Important

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

- Specify information for only one user on each line.

Example:

```
John,s8fK4br*,John's account,john@qnap.com
```

```
Jane,9fjwbXy#,Jane's account,jane@qnap.com
```

```
Mary,f9xn3nS%,Mary's account,mary@qnap.com
```

3. Save the list as a TXT file.



Important

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

Creating a CSV Domain User File

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

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



Important

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

Example:

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

3. Save the workbook as a CSV file.



Important

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

Batch Importing Domain Users

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



Important

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

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



Important

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

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

5. Click **Next**.
The **File content preview** screen appears.







Important

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

6. Click **Import**.
QTS imports the domain user account list.
7. Click **Finish**.

Modifying Domain User Account Information

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

| Task | User Action |
|----------------------------|--|
| Change password | <p>a. Under Action, click  . The Change Password window appears.</p> <p>b. Specify a password that meets the requirements.</p> <p>c. Verify the password.</p> <p>d. Click Change.</p> |
| 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. |

| Field | Description |
|-------|----------------------------|
| Type | Select the type of record. |

6. Modify the values.

| Task | User Action |
|-------------------|--|
| Add a value | <p>a. Specify a value.</p> <p>b.  Click . The value is added to the list.</p> |
| Move a value up | <p>a. Select a value from the list.</p> <p>b.  Click . The value moves up in the list.</p> |
| 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

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



Note

This is the account created when enabling the domain controller.

- Specify the following information.

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

- Click **Login**.

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

Adding Records

- 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**.

4. Services

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

Antivirus

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

Enabling Antivirus

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





Tip

- To update the antivirus now, click **Update now**.
 - To manually update the antivirus, click **Browse** and then select an updated file and click **Open**. After the file appears in the text box, click **Import**. You can download updated files from <http://www.clamav.net/>.
 - a. Select **Check and update automatically**.
 - b. Enter a number.
5. Click **Apply**.
QTS enables the antivirus.

Scanning Shared Folders

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

| Option | User Action |
|--------------------|----------------------------|
| All folders | Click All folders . |

| Option | User Action |
|-------------------------|--|
| 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 a file filter option.



Tip

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

10. Click **Next**.

The **Scan Options** screen appears.


11. Enter a maximum file size that Antivirus can scan.



Note

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

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


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

13. Click **Next**.

The **Action to take when infected files are found** screen appears.

14. Select an option on what to do with infected files.





| Option | Description |
|------------------------------|--|
| Only report the virus | QTS reports the virus but does not take any action on the detected files. The detections will appear in Reports . |

| Option | Description |
|--|---|
| Move infected files to quarantine | QTS quarantines the infected files. You cannot access these files from their shared folders. You can review the virus scan report in Reports and delete or restore infected files in Quarantine . |
|  Important These files are permanently deleted. | QTS deletes the infected files. |

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




Managing Scan Jobs

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

| Option | User Action |
|--------------------------|--|
| Run now | Select  . QTS starts the scan job. |
| Edit | <ol style="list-style-type: none"> a. Select . The Details window opens. b. Select the option you want to modify. c. After modifying the settings, click OK. QTS modifies the scan job's settings. |
| View last run log | <ol style="list-style-type: none"> a. Select . The Last run log window opens. b. Optional: Click the text box to modify the run log. c. Click Close. |
| Delete | Select  . QTS deletes the scan job. |

Managing Reported Scan Jobs

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > Antivirus > Reports** .
3. Locate the scan job you want to manage.
4. Under **Action**, select one of the following options.

| Option | User Action |
|-----------------|---|
| Download | Select  . QTS downloads the scan job as a text document to your computer.  Tip To download logs from all jobs, click Download All Logs at the lower right-hand corner of the screen. |
| Delete | a. Select  . A confirmation message appears. b. Click Yes . QTS deletes the scan job. |









Note

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

Managing Quarantine Files

- Log on to QTS as administrator.
- Go to **Control Panel > Applications > Antivirus > Quarantine**.
- Locate the file you want to manage.
- Under **Action**, select one of the following options.

| Option | User Action |
|--|--|
| Delete  Important You cannot recover deleted files. | Click  . QTS permanently deletes the file.  Tip <ul style="list-style-type: none"> You can delete multiple files on the list. Select the files you want to delete, and then click Delete Selected Files. You can delete all of the files on the list. To do so, click Delete All Files. |
| Restore | Click  . QTS restores the file to its shared folder.  Tip You can restore multiple files on the list. Select the files you want to restore, and at the top of the screen, select Restore Selected Files . |
| Exclude List | Click  . QTS restores the file to its shared folder and adds the file to the exclude list. |

Servers


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

Web Server

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

Enabling Web Server

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

| Setting | User Action |
|---|---|
| Enable HTTP compression | Select this option to improve transfer speeds and bandwidth utilization. |
| Enable secure connection (HTTPS) | <p>Select this option to allow HTTPS connections.</p> <ol style="list-style-type: none"> a. Select Enable secure connection (HTTPS). b. Optional: Select a TLS version. c. Specify a port number. d. Optional: Select Force secure connection (HTTPS) only to require all users to connect to the NAS using only HTTPS. |
| Maximum number of clients | <p>Enter a maximum client number.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note A client number is the number of users that are allowed to connect to the server. </div> |
| Do not allow Web Server embedding in IFrames | <ol style="list-style-type: none"> a. Select Do not allow Web Server embedding in IFrames. b. Optional: Add a website to allow Web Server embedding in IFrames. <ol style="list-style-type: none"> 1. Click Allowed Websites. The Allowed Websites window appears. 2. Click Add to add a website to the list. The Add Host Name window appears. 3. Specify a host name. 4. Click Add. The host name is added to the allowed websites list. 5. Click Apply. |

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

- Click **Apply**.


Tip

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

QTS enables Web Sever.

Modifying the php.ini Maintenance File

This task requires that you enable Web Server.

- Log on to QTS as administrator.
- Go to **Control Panel > Applications > Web Server**.
- Underneath **php.ini Maintenance**, select one of the following options.

| Option | User Action |
|----------------|--|
| Upload | <ol style="list-style-type: none"> Click Upload. The Upload php.ini window opens. Click Browse. The Open window opens. Select a php.ini file. Click Upload. QTS uploads the file. |
| Edit | <ol style="list-style-type: none"> Click Edit. The Edit php.ini window opens. Edit the php.ini file. Click Apply. QTS saves the changes. |
| Restore | <ol style="list-style-type: none"> Click Restore. A confirmation message appears. Click OK. QTS restores the default php.ini file. |

Enabling and Creating a Virtual Host

- Log on to QTS as administrator.
- Go to **Control Panel > Applications > Web Server > Virtual Host**.
- Select **Enable Virtual Host**.
- Click **Apply**.
You can now create a virtual host.
- Click **Create a Virtual Host**.

The **Advanced Options** window opens.

6. Enter a host name.
7. Select a root directory.
8. Select a protocol.
9. Enter a port number.
10. Click **Apply**.
The virtual host appears in the Host Name list.

Enabling WebDAV

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

Mounting a Shared Folder using WebDAV on Windows



Important

Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see [Enabling WebDAV](#).

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Windows computer as a network drive via WebDAV.

1. On your Windows computer, open File Explorer.
2. Right-click **This PC** and select **Map network drive**.
Map Network Drive window appears.
3. Specify the path of the shared folder that you want to access.



Tip

Follow the format `http://NAS_IP_address_or_host_name:port_number/shared_folder_name`. For example: `http://172.17.45.155:80/Public`.

4. Enable **Reconnect at sign-in** and **Connect using different credentials**.

5. Click **Finish**.
Windows Security window appears.
6. Specify your NAS login credentials.
7. Click **Connect**.



Tip

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

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using Windows File Explorer.

Mounting a Shared Folder Using WebDAV on Mac



Important

Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see [Enabling WebDAV](#).

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Mac as a network drive via WebDAV.

1. On your Mac, go to **Finder > Go > Connect to Server** .
The **Connect to Server** window appears.
2. Specify the path of the shared folder that you want to access.



Tip

Follow the format `http://NAS_IP_address_or_host_name:port_number/shared_folder_name`. For example: `http://172.17.45.155:80/Public`.

3. Click **Connect**.
4. Specify your NAS login credentials.
5. Click **Connect**.

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using macOS Finder.

Enabling LDAP Server

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > LDAP Server** .
3. Select **Enable LDAP Server**.
4. Enter a domain name.
5. Enter and verify the password.
6. Click **Apply**.

SQL Server

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

Enabling SQL Server

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



Important

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

- a. Underneath **Database Maintenance**, select **Change Root Password**. The **Change Root Password** window opens.
- b. Enter and confirm a password.
- c. Click **OK**.
QTS changes the root password, and a confirmation window opens.
- d. Click **OK**.
4. Select **Enable SQL server**.
5. Optional: Enable TCP/IP networking.



Tip

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

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



Note

The default port is 3306.

6. Click **Apply**.
QTS enables SQL server.

Reinitializing the Database

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > SQL server** .
3. Underneath **Database Maintenance**, click **Reinitialize Database**. The **Reinitialize Database** window opens.
4. Enter and confirm your SQL password.
5. Click **Reinitialize**.
QTS reinitializes the database and a confirmation message appears.

6. Click **OK**.

Syslog Server

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

Enabling Syslog Server

1. Log on to QTS 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. Underneath **Log Settings**, enter a number between 1-100 to specify the maximum log size.
 - b. Select the destination folder where you want to save the logs.
 - c. Enter the log file name.
6. Optional: Enable the email notification settings.



Note

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

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

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

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



Note

For details on configuring notification rules, 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 QTS as administrator.
2. Go to **Control Panel > Applications > Syslog Server > Filter Settings** .
3. Click **Add a Filter**.
The **Add a Filter** window opens.
4. Configure the filter.
 - a. Select the filter type.
 - **Facility**
 - **Severity**
 - **Hostname**
 - **Application**
 - **Message**
 - **IP**
 - b. Select a filter option.
 - **greater than or equal to**
 - **less than or equal to**
 - **equals**
 - **starts with**
 - **contains**
 - **not equals**
 - **not starts with**
 - **not contains**
 - c. Enter the filter condition.
 - d. Click **Add**.








Tip

- To remove an existing filter, click **Remove**.
 - To manually edit a filter, select **Manual Edit**.
- e. Click **Apply**.
QTS adds the Syslog filter.

Managing Syslog Filters

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > Syslog Server > Filter Settings** .
3. Locate the filter you want to modify.
4. Under **Action**, select one of the following options.

| Option | User Action |
|---|--|
| Enabled  Note This option only appears for disabled filters. | Click  . QTS enables the filter. |
| Disabled  Note This option only appears for enabled filters. | Click  . QTS disables the filter. |
| Edit | <ol style="list-style-type: none"> a. Click . The Filter window opens. b. Modify the filter. c. Click Apply. QTS saves the filter information. |



Tip

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

RADIUS Server

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

Enabling RADIUS Server

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



Note

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

5. Click **Apply**.






Creating a RADIUS Client

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

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

Managing RADIUS Clients

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > RADIUS Server > RADIUS Clients** .
3. Locate the client you want to modify.
4. Under **Action**, select one of the following options.

| Option | User Action |
|---|--|
| Enabled  Note This option only appears for disabled clients. | Click  . QTS enables the client. |
| Disabled  Note This option only appears for enabled clients. | Click  . QTS 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. QTS saves the client information. |



Tip

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






Creating a RADIUS User

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

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

Managing RADIUS Users

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > RADIUS Server > RADIUS Users** .
3. Under **Action**, select one of the following options.

| Option | User Action |
|---|---|
| Enabled  Note This option only appears for disabled users. | Click  . QTS enables the user. |
| Disabled  Note This option only appears for enabled users. | Click  . QTS 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. QTS saves the new password. |



Tip

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

Enabling TFTP Server

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

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



Note

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

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



Note

This option saves the TFTP log file. QNAP recommends viewing the log file using Microsoft Excel or WordPad on Windows or TextEdit on macOS.

- a. Select **Enable TFTP logging**.
 - b. Specify the folder where you want to save log files.
 - c. Specify the access right.
7. Select where to allow TFTP access.
 8. Click **Apply**.

Enabling NTP Server

This task allows the NTP Server to allow other network devices to synchronize their time with the NAS.

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

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

5. Click **Apply**.
QTS enables NTP Server.

5. File Station

Overview

About File Station

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

System Requirements

| Category | Detail |
|--------------|--|
| Web browser | <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. |

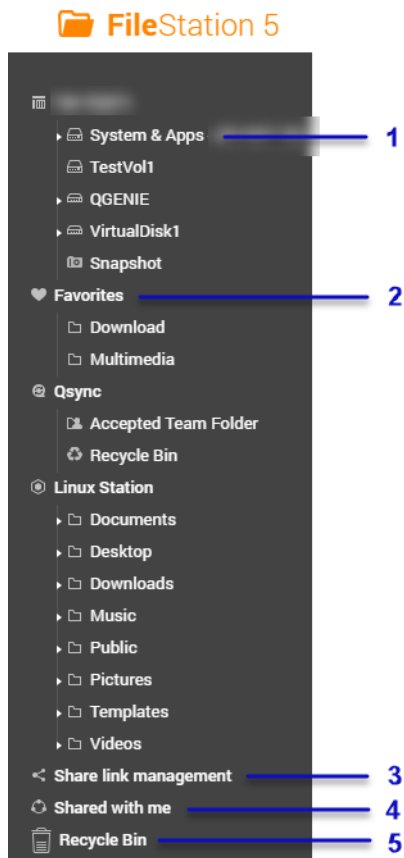
Supported File Formats


| 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 | Volume | Displays all the folders on the volume, including shared folders. Default shared folders vary depending on the NAS model. |
| 2 | Favorites | Displays bookmarked folders. |
| 3 | Share link management | Displays links to NAS files shared by the current user account.  Note Users in the administrator group can see links shared by all NAS users. |
| 4 | Shared with me | Displays files and folders shared with the current user account. |
| 5 | Recycle Bin | Displays deleted files and folders. |

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

| Folder | Description |
|----------------------------------|---|
| Snapshot | Displays the saved snapshots. |
| Local folders | Displays the local folders on a Windows computer.  Important To view local folders from File Station, you must first install Java Runtime Environment. |
| Qsync | Displays files, folders, and team folders from Qsync. |
| SMB shared folder | Displays files and folders from a shared folder mounted through SMB protocol.  Note To view the folder name, connection name, and the file protocol, hover your cursor over an SMB shared folder. |
| NFS shared folder | Displays files and folders from a shared folder mounted through NFS protocol.  Note To view the folder name, connection name, and the file protocol, hover your cursor over an NFS shared folder. |
| File Cloud Gateway shared folder | Displays files and folders from a shared folder mounted through a File Cloud Gateway connection via HybridMount. |

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

| Mount | Description |
|----------------|---|
| CIFS/SMB | Displays a list of connections mounted through CIFS/SMB protocol. |
| NFS | Displays a list of connections mounted through NFS protocol. |
| FTP | Displays a list of connections mounted through FTP protocol. |
| WevDAV | Displays a list of connections mounted through a local network or over the internet. |
| Cloud services | Displays a list of connections mounted through a cloud service.  Note To view the folder name, connection name, and the cloud provider, hover your cursor over the cloud mount. |

Left Panel Tasks

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



Tip






To see the task options, hover the mouse point over a volume and then click .

| Task | Description |
|------------------------|---|
| Create a shared folder | Click to create a shared folder. For details, see Creating a Shared Folder . |

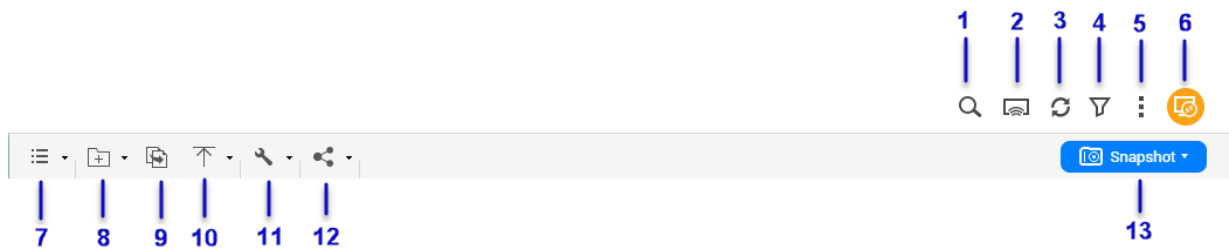
| Task | Description |
|------------------------|--|
| Open Snapshot Manager | Click to open Snapshot Manager. For details, see the Snapshots section of the QTS User Guide. |
| Lock/Unlock the volume | Click to lock or unlock an encrypted volume in Storage & Snapshots. |


Volume Icons




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

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

Toolbar




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

| Label | Item | Description |
|-------|---------------|---|
| 6 | Remote Mount | Manage files across local, external, remote, and cloud storage resources on a single interface. To use this feature, install HybridMount from App Center. For more information on HybridMount, go to the QNAP website. |
| 7 | Browsing Mode | Select a browsing mode. |
| 8 | Create folder | Create a folder, shared folder, snapshot 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. |
| 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. 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 |

5. Click **Apply**.
6. Click **Close**.

Modifying Third-party Service Settings

You can convert Apple iWork file formats to Microsoft Office file formats using CloudConvert. The converted files will be stored in the same folder with source files.

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


Tip

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

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

File Operations


File Station enables you to perform the following tasks.

| Operation | Task |
|-----------|---|
| Store | <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 • Playing a Video File Using CAYIN MediaSign Player • 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 | <p>a. Select the file.</p> <p>b.  Click .</p> <p>c. Select Edit with Office Online.</p> |
| 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 | <p>a. Select the file.</p> <p>b.  Click .</p> <p>c. Select Open with Image2PDF.</p> |
| 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 | <p>a. Select the file.</p> <p>b.  Click .</p> <p>c. Select Properties.</p> |
| Using the context menu | <p>a. Right-click the file.</p> <p>b. Select Properties.</p> |

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. |
| Volume | Displays the name of the volume on which the file is stored. |
| View Access Logs | Keeps track of access to the file.  Tip To enable this feature, click Start Logging in Control Panel > System > System Logs > System Connection Logs . |

4. Click **Close**.


Modifying File Permissions

This task requires that you enable advanced folder permissions in **Control Panel > Privilege > Shared Folders > Advanced Permissions** .

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

| Method | Steps |
|------------------------|---|
| 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 .


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. |

| Method | Steps |
|--------------------------|--|
| 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. |
| 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 | <p>a. Select the file.</p> <p>b.  Click .</p> <p>c. Select Copy to/Move to and then select Move to.</p> <p>d. Select the destination folder.</p> <p>e. Click OK.</p> |
| | <p>a. Select the file.</p> <p>b.  Click .</p> <p>c. Select Cut.</p> <p>d. Select the destination folder.</p> <p>e.  Click .</p> <p>f. Select Paste.</p> |
| 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 | <ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Rename. |
| Using the context menu | <ol style="list-style-type: none"> a. Right-click the file. b. Select Rename. |
| Use a keyboard shortcut | Press F2 . |

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

Deleting a File

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


| Method | Steps |
|------------------------|--|
| Using the toolbar | <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 | <ol style="list-style-type: none"> a. Select the file or folder. b. Click . c. Select Compress(Zip). |
| Using the context menu | <ol style="list-style-type: none"> a. Right-click the file or folder. b. Select Compress(Zip). |

4. Configure the file compression settings.


| Option | Task |
|-------------------|--|
| Archive name | Specify a name for the compressed file. |
| Compression level | Select the type of compression method. <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 |

| Option | Task |
|-------------|--|
| 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 |

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

Extracting Compressed Files or Folders

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


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

- 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.

Sharing a File or Folder by Email


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

- Open File Station.
- Locate the file or folder.
- 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 Via Email. |
| Using the context menu | <ol style="list-style-type: none"> a. Right-click the file or folder. b. Select Share. c. Select Via Email. |







The **Share** window appears.

4. Configure the following settings.

| Field | User Action |
|------------------|--|
| Send from | Select the email delivery method. <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 | Specify the email address of the recipient. <div style="margin-top: 10px;">  Tip You can select a recipient from your contact list if Qcontactz is installed on the NAS. </div> |
| Subject | Specify the email subject line. |
| Message | Enter a new message or use the default message. |

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

| Field | User Action |
|------------------|---|
| Link Name | Enter a name for the link or use the current name of the file or folder. <div style="margin-top: 10px;">  Note A link name cannot contain the following characters: / \ : ? < > * " </div> |

| 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</p> <ul style="list-style-type: none"> • You can choose to include the password in the email. • To show the password in the email, select Show the password in the email. |

6. Click Share Now.

File Station sends an email to the recipient.

Sharing a File or Folder on a Social Network

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


| Method | User Action |
|------------------------|--|
| Using the toolbar | <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>Enter a name for the link or use the current name of the file or folder.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Note</p> <p>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 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 | 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"> Select the file or folder. Click Share. Select Create share link only. |
| Using the context menu | <ol style="list-style-type: none"> Right-click the file or folder. Select Share and then select Create share link only. |




The **Share** window appears.

**Note**

You can share a maximum number of 100,000 files and folders. If a link shares one file or folder, you can create 100,000 share links. However, if a link shares 500 files or folders, you can only create 200 share links.

4. Configure the following 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> |
| 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. |

| Field | User Action |
|-------------------------------|---|
| 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</p> <p>This setting only appears when sharing folders.</p> |
| Expire in | <p>Specify the expiration date.</p> <p> Note</p> <p>This setting only appears when you share a folder.</p> |
| Password | <p>Require a password to access the link.</p> |

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 | <p>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.</p> <p> Note</p> <p>You can specify the email information for each user in Control Panel > Privilege > Users .</p> |

| Option | User Action |
|----------|----------------------------|
| New user | Create a new user account. |

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> |
| 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> |

| Field | User Action |
|-----------------|---|
| Password | Require a password to access the link.  Tip <ul style="list-style-type: none"> • If you enable this option, this field cannot be empty. • To show the password in the email, select Show the password in the email. |

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

Playing an Audio 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 Play. |
| Using the context menu | <ol style="list-style-type: none"> a. Right-click the file. b. Select Play. |

File Station plays the selected audio file using Media Viewer.

Playing a Video File

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

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

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

| | |
|--|-------------------------|
| | c. Select a resolution. |
|--|-------------------------|

File Station plays the selected file using Media Viewer.

Playing a Video File Using CAYIN MediaSign Player



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



Note

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

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

| Method | Steps |
|------------------------|---|
| Using the toolbar | <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 | <ol style="list-style-type: none"> a. Select the file. |



| | |
|------------------------|---|
| | <ol style="list-style-type: none"> 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. 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 | <ol style="list-style-type: none"> a. Select the file. b. Click . c. Select Cancel/Delete Transcoding. |
| Using the context menu | <ol style="list-style-type: none"> a. Right-click the file. b. Select Cancel/Delete Transcoding. |


A confirmation message appears.

4. Click **OK**.

File Station removes the selected file from the Transcode folder and cancels the transcoding process.

Viewing Transcode Information

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

| Method | Steps |
|------------------------|---|
| Using the toolbar | <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.

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 |


| Operation | Task |
|-------------|--|
| Share | <ul style="list-style-type: none"> • Creating a Shared Folder • Creating a Snapshot 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"> Select the folder. Click . Select Properties. |
| Use the context menu | <ol style="list-style-type: none"> Right-click the folder. Select Properties. |
| Use the left panel | <ol style="list-style-type: none"> Right-click the folder. Select Properties. |

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


| Field | Description |
|-------------------------------------|--|
| Type | Displays the folder type. |
| Size | Click  to display the folder size and total file count. |
| File Path | Displays the folder location. |
| 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. |
| Volume | Displays the name of the volume on which the folder is stored. |
| Transfer to Dedicated Volume | Migrates this shared folder to a snapshot shared folder. |
| View Access Logs | Keeps track of access to the folder.  Tip To enable this feature, select Track file and folder access in File Station > Options . |

| Field | Description |
|---------------------------|---|
| Multimedia Console | Opens Multimedia Console. This allows you to manage multimedia content sources. |
| Shared Folder | Edits folder properties. |

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. 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. |
| Volume | Displays the volume name. |
| Capacity | Displays the total storage capacity of the shared folder. |
| Free size | Displays the total available storage space in the shared folder. |
| Volume status | Displays the volume status. |


4. Click **Close**.

Modifying Folder Permissions


This task requires that you enable advanced folder permissions in **Control Panel > Privilege > Shared Folders > Advanced Permissions** .

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

| Method | Steps |
|-------------------|---|
| Using the toolbar | <ol style="list-style-type: none"> a. Select the folder. |

| | |
|------------------------|---|
| | <ol style="list-style-type: none"> 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




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.

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"> • Sharing a File or Folder by Email • Sharing a File or Folder on a Social Network • Sharing a File or Folder Using Share Links • Sharing a File or Folder with a NAS User |
| Stop sharing | Click  . |
| Copy the link to the clipboard | Click  . |

File Station performs the specified task.


Viewing Files and Folders Shared with Me

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

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

Creating a Folder

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


| Task | Steps |
|-------------------|--|
| 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. |

| Task | Steps |
|------------------------|--|
| 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 A Shared Folder** window opens.
4. Configure the folder settings.

| Field | Description |
|--------------------|---|
| Folder Name | Specify a folder name that contains 1 to 64 characters and that does not: <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: " + = / \ : * ? < > ; [] % ` ' . |


| Field | Description |
|---------------------------|--|
| Comment (optional) | Specify a comment that contains 1 to 128 ASCII characters. |
| Disk Volume | Specify the volume on which the shared folder will be created. |
| Qtier auto Tiering | Select this option to enable auto-tiering for this folder.  Note To use this feature, you must enable Qtier on the storage pool. |
| Path | <ul style="list-style-type: none"> • Specify path automatically: Creates a new root folder on the selected volume using the specified shared folder name. • Enter path manually: Select an existing folder as the root folder. |

5. Optional: Configure user access permissions.

- a. Under **Configure access privileges for users**, click **Edit**.
- b. Specify access permissions for each user.

6. Optional: Enable folder encryption.


- a. Under **Folder Encryption**, click **Edit**.
- b. Select **Encryption**.
- c. Specify the following information.

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

7. Optional: Configure advanced settings.


- a. Under **Advanced Settings**, click **Edit**.
- b. Configure the following settings.

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


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

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

Creating a Snapshot Shared Folder

- Open File Station.
- On the menu bar, click .
- Select **Snapshot shared folder**.
The **Create a Snapshot Shared Folder** window opens.
- Configure the folder settings.

| Field | Description |
|---------------------------|---|
| Folder Name | Specify a folder name that contains 1 to 64 characters and that does not: <ul style="list-style-type: none"> Begin or end with a space Contain consecutive spaces Contain the following characters: " + = / \ : * ? < > ; [] % ` ` '. |
| Comment (optional) | Specify a comment that contains 1 to 128 ASCII characters. |
| Storage Pool | Specify the storage pool where this shared folder will be created. |


| Field | Description |
|------------------------------|---|
| Space Allocation | Select one of the following space allocation options: <ul style="list-style-type: none"> • Thick provisioning • Thin provisioning |
| Qtier Auto Tiering | Select this option to enable auto-tiering for this folder. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note To use this feature, you must enable Qtier on the storage pool. </div> |
| Allocate Folder Quota | Specify a data quota for the folder. |


5. Optional: Configure user access permissions.
 - a. Under **Configure access privileges for users**, click **Edit**.
 - b. Specify access permissions for each user.
6. Optional: Configure advanced settings.
 - a. Under **Advanced Settings**, click **Edit**.
 - b. Configure the following settings.

| Option | Description |
|--|--|
| Guest Access Right | Select the permission level assigned to users without a NAS account. |
| Hide network drive | Selecting this option hides the folder in Windows networks. Users who know the specific path can still access the folder. |
| Lock File (Oplocks) | Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files. |
| SMB Encryption | This option is available only when SMB3 is enabled. Selecting this option encrypts all Microsoft network communication using the SMB3 protocol. |
| Enable Windows Previous Versions | Selecting this option allows users to use the Previous Versions feature on Windows to restore the previous versions of this shared folder. |
| Enable Network Recycle Bin | Selecting this option creates a Recycle Bin for this shared folder. |
| Restrict the access of Recycle Bin to administrators only for now | Selecting this option prevents non-administrator users from recovering or deleting files in the Recycle Bin. |
| Enable access-based share enumeration (ABSE) | When this option is enabled, users can only see the shared folders that they have permissions to mount and access. Guests must specify a username and password to view shared folders. |
| Enable access-based enumeration (ABE) | When this option is enabled, users can only see the shared folders that they have permissions to mount and access. |
| Set this folder as the Time Machine backup folder (macOS) | Selecting this option allows users to back up the data on the Mac to this shared folder via Time Machine. |

7. Click **Create**.
File Station creates a snapshot shared folder.

Sharing Space with a New User

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

| Field | Description |
|--|---|
| Username | Specify a username that contains 1 to 32 characters from any of the following groups: <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 QTS. |
| Email (optional) | QTS sends a notification to this email address when the account password is about to expire. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note</p> <ul style="list-style-type: none"> • You must configure the related settings in SMTP Server and Change Password. Otherwise, QTS would not send notifications to the specified email address. • SMTP Server: Go to Control Panel > System > Notification > E-mail . • Change Password: Go to Control Panel > System > Security > Password Policy . </div> |
| (Optional) Send a notification mail to the newly created user | When selected, QTS sends a message that contains the following information to the specified email address. <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 | <p>a. Click .</p> <p>b. Select Always Keep in Reserved Cache. A confirmation message appears.</p> <p>c. Click OK.</p> |
| Using the context menu | <p>a. Right-click the selected item.</p> <p>b. Select Always Keep in Reserved Cache. A confirmation message appears.</p> <p>c. Click OK.</p> |

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

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

| Status Icon | Description |
|---|--|
|  | This file or folder is only stored in the cloud |
|  | File Station is downloading this file or folder. |
|  | File Station has encountered an error when downloading this file or folder. |
|  | File Station has cached and is uploading this file or folder. |
|  | File Station has cached and placed this file or folder in the upload queue. |
|  | File Station has encountered an error when uploading this file or folder. |
|  | This file or folder has been cached and synced and will always be kept in the reserved cache. |
|  | This file or folder has been cached and synced. |
|  | This file or folder has been cached and synced but marked as low priority. When the cache space is insufficient, File Station will remove files or folders that are the least recently accessed. |
|  | This file or folder is ignored and not uploaded to the cloud. File Station ignores and skips temporary system files during the sync process. |

Removing a Folder from Reserved Cache

You can remove folders from the reserved cache.




Important

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

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

4. Choose one of the following methods.

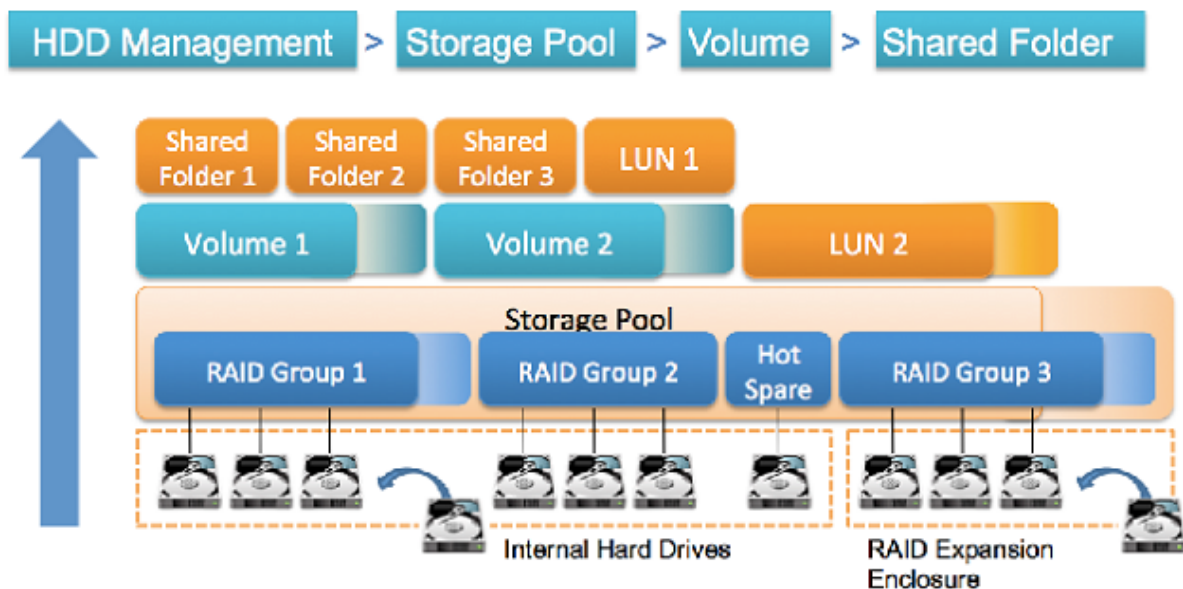
| Method | Steps |
|------------------------|--|
| Using the toolbar | <p>a. Select one or more folders.</p> <p>b. Click .</p> <p>c. Select Do Not Keep in Reserved Cache. A confirmation message appears.</p> <p>d. Click OK.</p> |
| Using the context menu | <p>a. Select one or more folders.</p> <p>b. Right-click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

6. Storage & Snapshots

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


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

QTS Flexible Volume Architecture



QTS Flexible Volume Architecture


| Object | Description | Details |
|--------------|--|--|
| Disk | A physical device that stores and retrieves data. | QTS restricts which type of disk can be used for SSD cache and storage space (static volumes and storage pools). For details, see Disk Types . |
| RAID group | A group of one or more disks combined into one logical disk. RAID groups usually contain disks that are of the same type and capacity. | Data is distributed across the disks in a RAID group. Each RAID type offers a different combination of reliability, performance, and capacity. For details, see RAID . |
| Storage pool | A pool of storage space consisting of one or more RAID groups. | Storage pools can aggregate RAID groups that consist of disks of different types and capacities. Storage pools enable easier storage space management and features such as snapshots. |



| Object | Description | Details |
|---------------------------------|---|--|
| Volume | A portion of storage space that is used to divide up and manage space on the NAS. | <p>You can create volumes by dividing up storage pool space, or using the space of a RAID group. QTS offers three different volume types, with different combinations of performance and flexibility.</p> <p> Important You must create at least one volume before the NAS can start storing data.</p> |
| iSCSI LUN (logical unit number) | A portion of storage space that can be used by other NAS devices, servers and desktop computers using the iSCSI protocol. | <p>QTS offers two LUN types.</p> <ul style="list-style-type: none"> • Block-based LUN: Created from a storage pool. It is similar to a volume, except that it has no file system and must be linked to an iSCSI host. • File-based LUN: Created on a volume. It is similar to an ISO image file. |
| Shared folder | A folder that is used for storing and sharing files. | <p>Shared folders are created on volumes. QTS automatically creates a set of default shared folders. You can create more shared folders and configure permissions for each.</p> |

Global Settings

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



Storage Global Settings

| Setting | Description |
|----------------------|---|
| RAID Resync Priority | <p>Specify the minimum speed of the following RAID operations:</p> <ul style="list-style-type: none"> • Rebuild • Migration • Scrubbing • Sync <p>You can select one of the following priorities:</p> <ul style="list-style-type: none"> • Service First: QTS performs RAID operations at lower speeds in order to maintain NAS storage performance. • Default: QTS performs RAID operations at the default speed. • Resync First: QTS performs RAID operations at higher speeds. Users may notice a decrease in NAS storage performance while RAID operations are in progress. <p> 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.</p> |


| Setting | Description |
|------------------------------------|--|
| RAID Scrubbing Schedule | Enable this feature to periodically scan for and fix bad sectors on RAID 5 and RAID 6 groups. |
| Auto Reclaim and SSD Trim Schedule | <p>Enable this feature to periodically run the following operations on all thin volumes and SSDs:</p> <ul style="list-style-type: none"> • Auto Reclaim: QTS returns unused storage space to the parent storage pool when files are deleted from thin volumes. • SSD Trim: QTS tells the SSD firmware which data blocks it is safe to erase when performing garbage collection. This helps maintain the SSD's write performance and lifespan. <p>By default, the operations are scheduled to run daily at 2:00 AM. SSD Trim is only performed on solid state drives that belong to a RAID 0, RAID 1, or RAID 10 group.</p> <p> Tip You should enable this feature if you have one or more of the following storage items:</p> <ul style="list-style-type: none"> • Thin volumes • SSD RAID groups of type: Single, RAID 0, RAID 1, RAID 10 <p> Note To reclaim space on a thin LUN, the reclaim must be run on the iSCSI client.</p> |
| Scheduled File System Check | Enable this feature to scan and automatically fix all volumes that have file system errors at a later date. |

Disk / Device Global Settings

| Setting | Description |
|---|---|
| Activate Predictive S.M.A.R.T. Migration | Enable this feature to regularly monitor disk health. If S.M.A.R.T. errors are detected on a disk, QTS displays a warning and then begins migrating data from the faulty disk to a spare disk. After the migration is finished, the healthy disk is used in place of the faulty disk. This process is safer than manually initiating a full RAID rebuild after a disk has failed. |
| Use SSD estimated remaining life with S.M.A.R.T. disk migration | Enable this feature to migrate data from an SSD to a spare disk and rebuild the RAID group when the SSD's estimated remaining life falls below 5%. |
| S.M.A.R.T. polling time | Specify how often QTS checks disks for S.M.A.R.T. errors in minutes. |
| Disk Temperature Alarm | Enable this feature to monitor the disk temperatures. QTS displays a warning when the disk temperature is equal to or above the specified threshold. You can set separate thresholds for hard disk drives and solid state drives. |

| Setting | Description |
|--|---|
| TLER/ERC Timer | <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. QTS might interpret this unresponsiveness as a disk failure. Enabling this feature ensures that a disk has sufficient time to recover from a read or write error before QTS marks it as failed and initiates a RAID group rebuild.</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, QTS uses the default TLER/ERC settings specified by the disk manufacturer. |
| Check for expansion unit firmware updates at login | <p>Enable this feature to automatically check online for newer firmware for each expansion unit connected to the NAS. If QTS detects newer firmware, it will ask whether you want to install it.</p> |
| 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 choose to exclude the most recent snapshot, or snapshots that were created with the setting Keep this snapshot permanently.</p> <p> Important</p> <p>If QTS is unable to create 32GB of free snapshot space, it will not create any new snapshots.</p> |
| 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> |
| Make snapshot directory (@Recently-Snapshot) visible in shared folder root | <p>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.</p> |

| Setting | Description |
|--|---|
| When the number of snapshots reaches maximum | Specify the default QTS behavior after a volume, LUN, or NAS reaches its maximum number of snapshots. You can choose one of the following behaviors: <ul style="list-style-type: none"> • Overwrite the oldest snapshot when taking a new one. • Stop taking snapshots. |
| Use timezone GMT+0 for all new snapshots | Enable this feature to use the GMT+0 time zone in the file names of new snapshots. This file naming convention can simplify snapshot management especially when working with snapshots from NAS devices located in different time zones. This setting only applies to new snapshots. Existing snapshots are not renamed. |
| Show hidden files in Snapshot Manager | Enable this feature to display hidden files in Snapshot Manager. This setting does not affect files inside the File Station Snapshot Directory. |
| Enable Windows Previous Versions | When enabled, Windows users can view and restore files from snapshots using the Previous Versions feature in Windows. You can disable this feature for individual folders by modifying the folder's properties. |

Storage

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

Disks

Disk Types

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



Important

- For compatibility reasons, PCIe form-factor SSDs and PCIe M.2 SSDs installed in third-party adapter cards cannot be used to create storage pools and static volumes.
- If you are already using NVMe PCIe SSDs for data storage, then your existing storage configuration will not be affected after upgrading to the latest version of QTS.

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


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 | QTS has detected S.M.A.R.T. errors. Run a full S.M.A.R.T. test and a disk scan. |
| Error | QTS has detected I/O errors. You must replace the disk immediately. |
| 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: QTS has detected an error. Run a full S.M.A.R.T. test and a disk scan. • Error: QTS has detected a critical error. You must replace the disk immediately. |
| Manufacturer | The manufacturer of the disk |
| Model | The disk model |
| Disk Capacity | <p>The capacity of the disk, in both binary and decimal formats</p> <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 QTS. • Decimal format assumes that 1 GB = 1,000,000,000 bytes. This format is used by disk manufacturers and appears in advertising, on the disk's box, and in the disk's hardware specifications. • Due to differences in the number of bytes per gigabyte, a disk's binary capacity will be slightly lower than its decimal capacity. For example, a disk advertised as 500 GB (decimal) has a true capacity of 456 GB (binary). |
| Bus Type | The interface that the disk uses |


| Information | Description |
|---------------------------|--|
| 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: QTS has not detected any I/O errors on the disk. • Error: QTS has detected one or more I/O errors on the disk. |
| Disk SMART Information |  Important If any of the S.M.A.R.T. attribute values reach the threshold set by the disk manufacturer or a predefined threshold determined by QTS, this field will change to Warning. |
| Estimated Life Remaining | The remaining life of the disk, as calculated by the disk's firmware. When the value reaches 0, you should replace the disk. This information is only available for solid-state drives (SSDs). |

Disk Actions

| Action | Description |
|------------------------|---|
| Disk Info | Displays disk details, including the disk manufacturer, model, serial number, disk capacity, bus type, firmware version, ATA version, and ATA standard. |
| Disk Health | Displays disk S.M.A.R.T. information. For details, see Disk Health Information . |
| Scan for Bad Blocks | Scan the disk for bad blocks.  Tip Run this scan if the disk's status changes to <code>Warning</code> or <code>Error</code> . If QTS does not detect any bad blocks, the status changes back to <code>Ready</code> . To view the number of bad blocks, see Disk Health > Summary . |
| Locate | Prompt the drive LEDs to blink so that you can locate the drive in a NAS or expansion unit. |
| Detach | Remove the disk from its RAID group. The group must be of type: RAID 1, RAID 5, RAID 6, RAID 10. |
| Set as Enclosure Spare | Assign the disk as a global hot spare for all RAID groups within the same enclosure (NAS or expansion unit). For details, see Configuring an Enclosure Spare Disk . |
| Disable Spare | Unassign the disk as a global hot spare. |
| New Volume | Create a new volume. For details, see Volume Creation . |
| Secure Erase | Permanently erase all data on a disk. For details, see Secure Erase . |
| RAID Group | Select a RAID group to view its RAID type, capacity, and member disks. |

Disk Health Information

| Tab | Description | Actions |
|----------------------------|--|---|
| Summary | Displays an overview of S.M.A.R.T. disk information and the results from the most recent disk scan and S.M.A.R.T. test. | - |
| 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. | - |
| 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 QTS, the SMART attribute's status will change to <code>Warning</code>.</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. |

| Tab | Description | Actions |
|----------|--|---|
| Settings | Disk settings can be applied individually, or to multiple disks at once. | Configure the following settings: <ul style="list-style-type: none"> • Enable temperature alarm: QTS displays a warning when the disk temperature is equal to or above the specified threshold. • S.M.A.R.T. Test schedule: Schedule periodic rapid and complete S.M.A.R.T. disk tests. The results are displayed on the Summary screen. • IronWolf Health Management: Schedule a daily IHM test for the disk. The results are saved in the selected shared folder, and are displayed on the IronWolf Health Management screen. <div style="border-left: 2px solid orange; padding-left: 10px; margin-top: 10px;">  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). </div> |

Disk Performance Tests

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



Important

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

Testing Disk Performance Manually

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

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

A confirmation message appears.

5. Click **OK**.

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

Testing Disk Performance on a Schedule

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

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

Secure Erase

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


Securely Erasing a Disk



Important

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

1. Go to **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>QTS writes over all blocks on the disk with zeros or ones. This mode is the most secure but can take a long time to finish.</p> <p>Select Customized to configure the following the erase settings.</p> <ul style="list-style-type: none"> • Number of rounds: QTS writes over all blocks on the disk the specified number of times. • Overwrite with: Overwrite all blocks with zeros, ones, or a random zero or one. |
| SSD | <p>QTS issues a solid state drive (SSD) secure erase ATA command. The SSD firmware then erases all data and restores the disk to its original factory performance.</p> <p> Important This feature is only supported on specific SSD models.</p> |
| Fast | <p>QTS overwrites the partition and RAID configuration data on the disk with zeros. This mode is the quickest but is less secure than the other modes.</p> |

7. Click **Next**.

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

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

Volumes

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



Tip

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

Volume Types

Thick, Thin, and Static Volumes

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

| | Volume Type | | |
|---|---|--|---|
| | Static | Thick | Thin |
| Effect of data deletion | Space is freed in the volume | Space is freed in the volume | QTS can reclaim the space and add it back into the parent storage pool. |
| Method of adding storage space | <ul style="list-style-type: none"> • Add disks to the NAS • Replace existing disks with higher capacity disks | Allocate more space from the parent storage pool | Allocate more space from the parent storage pool |
| Snapshot support (fast backup and recovery) | No | Yes | Yes |
| Qtier (automatic data tiering) support | No | Yes | Yes |

Legacy Volumes

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

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

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



Tip

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

The System Volume

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



Important

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

The screenshot shows the 'Storage & Snapshots' management interface. At the top, there are tabs for 'External Storage Devices', 'SSD Over-Provisioning', 'Qtier', and 'VJBOD/VJBOD Cloud'. Below these, a 'Storage Space' section shows 'Storage Pool: 1, Volume: 4, LUN: 2'. A table lists the following volumes:

| Name/Alias | Status | Type | Snapshot | Snapshot ... | Capacity | Percent Used |
|-----------------------|------------------|------------------------|----------|--------------|-----------|----------------|
| Storage Pool 1 | | | | | | |
| DataVol1 | Ready (Check...) | Thick volume | -- | -- | 75.38 GB | [Progress bar] |
| HybridMount1 | Ready | Thick Stored Space | -- | -- | 95.85 GB | [Progress bar] |
| HybridMount2 | Ready | Thick Stored Space | -- | -- | 95.85 GB | [Progress bar] |
| LUN_1 (Mappe... | Ready | Block-based Thin L... | -- | -- | 5.00 GB | [Progress bar] |
| LUN_2test (Ma... | Ready | Block-based Thick L... | -- | -- | 1.00 GB | [Progress bar] |
| Static Single Volu... | | | | | | |
| SYSTEM DO -- | Ready (Check...) | Static volume | -- | -- | 446.55 GB | [Progress bar] |

Volume Configuration

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

| Configuration | Advantage | Description |
|--|------------|---|
| Single Volume Example: | Simplicity | Creating one volume is quick and easy. After the initial setup, you do not have to worry about changing volume sizes or creating new volumes. |
| <ul style="list-style-type: none"> • Volume 1 <ul style="list-style-type: none"> • Shared Folder 1 • Shared Folder 2 • Shared Folder 3 • Shared Folder 4 | Speed | Single static volumes are faster because they do not require a storage pool. |

| Configuration | Advantage | Description |
|---|-----------------------------|--|
| Multiple Volumes Example: <ul style="list-style-type: none"> • Volume 1 <ul style="list-style-type: none"> • Shared Folder 1 • Volume 2 <ul style="list-style-type: none"> • Shared Folder 2 • Volume 3 <ul style="list-style-type: none"> • Shared Folder 3 • Volume 4 <ul style="list-style-type: none"> • Shared Folder 4 | Storage space limits | Each volume functions like a separate container. If a user or an app writes a large amount of files to a volume, only the specified volume is filled. Other volumes remain unaffected. |
| | Multiple snapshot schedules | Snapshots protect files from accidental deletion or modification. Snapshot creation requires time, memory resources, and storage space. QTS takes snapshots of individual volumes. Using multiple volumes means you can have different snapshot schedules for different file types. For example, you can take hourly snapshots of the volume containing important documents, and weekly snapshots of the volume contain photos and movies. |
| | Faster file system repair | In certain circumstances such as after a power outage, QTS may encounter errors in the file system of a volume. While QTS can scan the volume and automatically repair errors, this process can take a long time. The required time depends on the volume size. Files on the volume cannot be accessed during the scanning process. |

Volume Configuration Examples

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

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

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

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

Volume Creation

Creating a Static Volume

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

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

The **Volume Creation Wizard** window opens.

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



Important

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

6. Select one or more disks.




Important

- For data safety, you cannot select disks that have the status `Warning`.
- The status `In Use` means that a disk is currently formatted as an external disk, and may contain current user data.
- If you select a disk with the status `In Use`, QTS will temporarily stop all disk storage services on the NAS in order to unmount the disk, and then delete all data and partitions on the disk.

**Warning**

All data on the selected disks will be deleted.

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

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

**Tip**

Use the default RAID type if you are unsure of which option to choose.
For details, see [RAID Types](#).

- Optional: Select the disk that will be used as a hot spare for this RAID group.
The designated hot spare automatically replaces any disk in the RAID group that fails.
For details, see [RAID Disk Failure Protection](#).
- 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.

- Click **Next**.
- Optional: Specify an alias for the volume.
The alias must consist of 1 to 64 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Hyphen (-), underscore (_)
- Optional: Configure SSD over-provisioning.

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



Tip

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

13. Specify the number of bytes per inode.

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

14. Optional: Configure advanced settings.

| Setting | Description | User Actions |
|---------------------------------------|--|---|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |
| Encryption | QTS encrypts all data on the volume with 256-bit AES encryption. | <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 QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  Warning <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> |
| Accelerate performance with SSD cache | QTS adds data from this volume to the SSD cache to improve read or write performance. | No actions |

| Setting | Description | User Actions |
|--------------------------------------|---|---|
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | <ul style="list-style-type: none"> Specify a folder name. Select Create this folder as a snapshot shared folder. <p>A snapshot shared folder enables faster snapshot creation and restoration.</p> |

15. Click **Next**.

16. Click **Finish**.

A confirmation message appears.



Warning

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

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

Creating a Thick or Thin Volume

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

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

The **Volume Creation Wizard** window opens.

3. Select the volume type.

- Thick Volume
- Thin Volume

For details, see [Volumes](#).

4. Select a storage pool.

You can select an existing storage pool or create a new storage pool immediately.

5. Optional: Create a new storage pool.

a. Click .

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

b. Click **Next**.

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



Important

- You cannot select disks from multiple expansion units.

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


d. Select one or more disks.



Warning

All data on the selected disks will be deleted.

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

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



Tip

Use the default RAID type if you are unsure of which option to choose.
For details, see [RAID Types](#).

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



Tip

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

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

**Warning**

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

m. Click **OK**.

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

6. Click **Next**.

7. Optional: Specify an alias for the volume.

The alias must consist of 1 to 64 characters from any of the following groups:

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

8. Specify the capacity of the volume.

The volume type determines the maximum volume capacity.

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


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

9. Specify the number of bytes per inode.

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

10. Optional: Configure advanced settings.

| Setting | Description | User Actions |
|-----------------|--|------------------|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |

| Setting | Description | User Actions |
|---------------------------------------|---|---|
| Encryption | QTS 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 QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts. <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. |
| Accelerate performance with SSD cache | QTS adds data from this volume to the SSD cache to improve read or write performance. | |
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | <ul style="list-style-type: none"> Specify a folder name. Select Create this folder as a snapshot shared folder. <p>A snapshot shared folder enables faster snapshot creation and restoration.</p> |

11. Click **Next**.

12. Click **Finish**.

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

Volume Management

Deleting a Volume



Note

- To delete a VJBOD Cloud volume, use the VJBOD Cloud app.
- To delete a HybridMount volume, use the HybridMount app.

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



Warning

All data on the selected volume will be deleted.

3. Click **Manage**.
4. Select **Remove > Remove Volume** .
The **Volume Removal Wizard** window opens.
5. Click **Apply**.

Configuring a Volume Space Alert

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

Volume File System Check

A file system check scans for and automatically repairs errors in the file system of a thick, thin, or static volume. QTS will prompt you to start a file system check if it detects file system errors on one or more volumes. You can also run a file system check manually or schedule a one-time check.

Running a File System Check Manually



Warning

- A volume is unmounted and becomes inaccessible while its file system is being checked.
- This process might take a long time, depending on the size of the volume.



Important

QTS will scan the specified volume, even if QTS has not detected any errors on the volume's file system.

1. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a volume.
3. Click **Manage**.
The **Volume Management** window opens.
4. Click **Actions**, and then select **Check File System**.
The **Check File System** window opens.
5. Click **OK**.

QTS creates a background task for the file system check. The status of the volume changes to *Checking...*

Running a One-Time File System Check on a Schedule





Warning

- A volume is unmounted and becomes inaccessible while its file system is being checked.
- This process might take a long time, depending on the size of the volume.



Important

QTS will only scan the specified volume if it has detected errors on the volume's file system.

1. Open **Storage & Snapshots**.
2.  Click . The **Global Settings** window appears.
3. Click **Storage**.
4. Enable **Scheduled File System Check**.
5. Specify a date and time.
6. Click **Apply**.

Volume Expansion


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

Resizing a Thick or Thin Volume

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

| Operation | Details |
|---------------|---|
| Expand Volume | <ul style="list-style-type: none"> • The operation can be performed while the volume is online and accessible to users. • For a thick volume, additional space is allocated from the volume's parent storage pool. |
| Shrink Volume | <ul style="list-style-type: none"> • Users and applications will be unable to access the volume until the operation is finished. • For a thick volume, the freed space is returned to the volume's parent storage pool. |

| Volume Type | Maximum Allowed Capacity |
|-------------|--|
| Thick | Amount of free space in the parent storage pool. |

| Volume Type | Maximum Allowed Capacity |
|-------------|---|
| Thin | <p>Twenty times the amount of free space in the parent storage pool.</p> <div style="display: flex; align-items: flex-start;">  <p>Important Setting the maximum size of a thin volume to a value that is greater than the amount of free space in the storage pool is called over-allocation.</p> </div> |

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

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

Expanding a Static Volume by Adding Disks to a RAID Group

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



Important

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

1. Verify the following:
 - The storage pool you want to expand contains at least one RAID group of type: RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60.
 - The NAS contains one or more free disks. Each free disk must be the same type as the other disks in the RAID group (either HDD or SSD), and have a capacity that is equal to or greater than the smallest disk in the group.
 - The status of the RAID group that you want to expand is `Ready`.
2. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .

3. Select a static volume.
4. Click **Manage**.
The **Volume Management** window opens.
5. Click **Expand**.
The **Expand Static Volume Wizard** window opens.
6. Select **Add new disk(s) to an existing RAID group**.
7. Select a RAID group.
The group must be of type: RAID 1, RAID 5, RAID 6, RAID 50, RAID 60.
8. Click **Next**.
9. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

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

**Tip**

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

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

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

Expanding a Single Static Volume By Adding a New RAID Group

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

**Warning**

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

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

**Important**

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

8. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

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

**Important**

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

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

**Tip**

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

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

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

Storage Pools

A storage pool combines many physical disks into one large pool of storage space. Disks in the storage pool are joined together using RAID technology to form RAID groups. Storage pools may contain more than one RAID group.

Using storage pools provides the following benefits:

- Multiple volumes can be created in a storage pool, enabling you to divide the storage space among different users and applications.
- Disks of different sizes and types can be mixed into one large storage space.
- Disks from connected expansion units can be mixed with disks installed in the NAS to form a storage pool.
- Extra disks can be added while the storage pool is in use, increasing storage capacity without interrupting services.
- Qtier provides auto-tiering when a storage pool contains a mix of SATA, SAS, and SSD disks. Qtier automatically moves frequently accessed hot data to the faster SSDs, and infrequently accessed cold data to the slower disks.
- Snapshots can be used with storage pools. Snapshots record the state of the data on a volume or LUN at a specific point in time. Data can then be restored to that time if it is accidentally modified or deleted.
- Multiple RAID 5 or RAID 6 groups can be striped together using RAID 0 to form a RAID 50 or RAID 60 storage pool.

Creating a Storage Pool

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

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

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

3. 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


- For data safety, you cannot select disks that have the status `Warning`.

- The status `In Use` means that a disk is currently formatted as an external disk, and may contain current user data.
- If you select a disk with the status `In Use`, QTS will temporarily stop all disk storage services on the NAS in order to unmount the disk, and then delete all data and partitions on the disk.

**Warning**

All data on the selected disks will be deleted.

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

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

**Tip**

Use the default RAID type if you are unsure of which option to choose.
For details, see [RAID Types](#).

7. Optional: Select the disk that will be used as a hot spare for this RAID group.
The designated hot spare automatically replaces any disk in the RAID group that fails.
For RAID 50 or RAID 60, a spare disk must be configured later. You should configure a global spare disk so that all subgroups share the same spare disk.
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 SSD over-provisioning.

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



Tip

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

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

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

Storage Pool Management

Deleting a Storage Pool

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 **Confirm the removal of every volume/iSCSi LUN/Snapshot Vault on this storage pool**.



Warning

All data in the storage pool will be deleted.


6. Click **OK**.
The **Remove Pool** window opens.
7. Enter the admin password.
8. Click **OK**.

Configuring a Storage Pool Space Alert

1. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a storage pool.
3. Click **Manage**.
The **Storage Pool Management** window opens.
4. Click **Actions**, and then select **Set Threshold**.
The **Alert Threshold** window opens.
5. Enable space alerts.

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

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 QTS 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> . QTS 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> . <div style="display: flex; align-items: flex-start;">  <div> <p>Note It might be possible to recover some data from volumes and LUNs.</p> </div> </div> |

Storage Pool Expansion

Expanding a Storage Pool By Adding a New RAID Group

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



Warning

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

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

**Important**

- You cannot select disks from multiple expansion units.
- You cannot use the disks from a QNAP JBOD enclosure to expand a storage pool which is located on a different enclosure.
- If the expansion unit is disconnected from the NAS, the storage pool becomes inaccessible until it is reconnected.

8. Select one or more disks.

**Warning**

All data on the selected disks will be deleted.

9. Select a RAID type.

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

**Important**

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

10. Optional: Select the disk that will be used as a hot spare for this RAID group.
The designated hot spare automatically replaces any disk in the RAID group that fails.

11. Click **Next**.

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

**Tip**

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

13. Click **Next**.

14. Click **Expand**.
A confirmation message appears.

15. Click **OK**.

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

Expanding a Storage Pool by Adding Disks to a RAID Group

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

**Important**

- Adding disks to a RAID 1 group changes the RAID type of the group to RAID 5.

- To expand a RAID 50 or RAID 60 group, every sub-group must be expanded with the same number of disks.

1. Verify the following:

- The storage pool you want to expand contains at least one RAID group of type: RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60.
- The NAS contains one or more free disks. Each free disk must be the same type as the other disks in the RAID group (either HDD or SSD), and have a capacity that is equal to or greater than the smallest disk in the group.
- The status of the RAID group that you want to expand is *Ready*.

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

3. Select a storage pool.

4. Click **Manage**.

The **Storage Pool Management** window opens.

5. Select **Expand Pool > Expand Pool** .

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

6. Select **Add new disk(s) to an existing RAID group**.

7. Select a RAID group.

The group must be of type: RAID 1, RAID 5, RAID 6, RAID 50, RAID 60.

8. Click **Next**.

9. Select one or more disks.



Warning

All data on the selected disks will be deleted.

10. Click **Next**.

11. Optional: Configure SSD over-provisioning.

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



Tip

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

12. Click **Next**.

13. Click **Expand**.

A confirmation message appears.

14. Click **OK**.

15. Optional: For a RAID 50 or RAID 60 pool, repeat these steps for each sub-group.

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

Storage Pool Migration

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

- Files and folders
- Storage configuration
- Snapshots

Storage Pool Migration Requirements

The following requirements apply when migrating a storage pool to a new NAS.

- The two NAS devices must both be running QTS, or both be running QuTS hero. QTS to QuTS hero migration is not possible.
- The version of QTS or QuTS hero running on the new NAS must be the same or newer than the version running on the original NAS.

Migrating a Storage Pool to a New NAS

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

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

RAID

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

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

| RAID Feature | Description | Advantages | Disadvantages |
|--------------|---|--|---|
| Grouping | Disks that are combined using RAID form a RAID group, which QTS considers one large logical disk. | Managing the storage space of one large disk is simpler and more efficient than multiple small disks. | Initial configuration can be more complicated. |
| Striping | Data is split into smaller pieces. Each piece is stored on a different disk in the RAID group. QTS can then access that data by reading from or writing to multiple disks simultaneously, increasing read and write speeds. | <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 | Each disk in the RAID group can store the following: <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

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



Important

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

| RAID Type | Number of Disks | Disk Failure Tolerance | Capacity | Overview |
|------------------------------|-----------------|------------------------|--|---|
| Single | 1 | 0 | Total disk capacity | <ul style="list-style-type: none"> • Uses a single disk for storage. • Provides no disk failure protection or performance benefits. • Suitable for single disk configurations that have a data backup plan in place. |
| JBOD (just a bunch of disks) | ≥ 2 | 0 | Total combined disk capacity | <ul style="list-style-type: none"> • Combines disks together in a linear fashion. QTS writes data to a disk until it is full before writing to the next disk. • Uses the total capacity of all the disks. • Not a real RAID type. It provides no disk failure protection or performance benefits. • Unless you have a specific reason to use JBOD, you should use RAID 0 instead. |
| RAID 0 | ≥ 2 | 0 | Total combined disk capacity | <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. • Recommended for high-performance applications such as video editing. |
| RAID 1 | 2 | 1 | Half of the total combined disk capacity | <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 NAS devices with two disks. |

| RAID Type | Number of Disks | Disk Failure Tolerance | Capacity | Overview |
|-----------|---------------------------------|------------------------|--|--|
| RAID 5 | ≥ 3 | 1 | Total combined disk capacity minus 1 disk | <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. |
| RAID 6 | ≥ 4 | 2 | Total combined disk capacity minus 2 disks | <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 10 | ≥ 4 (Must be an even number) | 1 per pair of disks | Half of the total combined disk capacity | <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 | Total combined disk capacity minus 1 disk per 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. • Better random access performance than RAID 5 if all of the disks are SSDs. • Recommended for enterprise backup with ten or more disks. |

| RAID Type | Number of Disks | Disk Failure Tolerance | Capacity | Overview |
|-----------|-----------------|------------------------|---|---|
| RAID 60 | ≥ 8 | 2 per disk subgroup | Total combined disk capacity minus 2 disks per 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. Better random access performance than RAID 6 if all of the disks are SSDs. Recommended for business storage and online video editing with twelve or more disks. |

RAID Group Status

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

RAID Disk Failure Protection

All RAID types except for RAID 0 can tolerate a specific number of disk failures without losing data. When a disk in a RAID group fails, the RAID group status changes to `degraded` and then QTS performs one of the following actions.

| Spare Disk Available | Actions |
|----------------------|--|
| Yes | <ul style="list-style-type: none"> QTS automatically replaces the failed disk with a spare disk and then starts rebuilding the RAID group. The status of the RAID group changes to <code>rebuilding</code>, and then changes back to <code>Ready</code> after rebuilding has finished. |
| No | You must replace the failed disk manually. QTS starts rebuilding the RAID group after you have installed a working disk. |

Configuring a RAID Group Hot Spare

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

1. Verify that the NAS contains one or more free disks.

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



Warning

All data on the selected disks will be deleted.

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

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

Configuring 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.

RAID Bitmaps

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

A disk can become temporarily disconnected in the following situations.

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



Important

- You can only create bitmaps for RAID 1, RAID 5, RAID 6, and RAID 10 groups.
- Enabling a RAID bitmap may slightly decrease the read and write performance of the RAID group.
- A bitmap improves synchronization time only if the same disk is disconnected then reconnected. Having a bitmap does not improve synchronization time when a new disk is added to the RAID group.

Creating a RAID Bitmap

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

QTS creates a bitmap for the RAID group.

RAID Management

Expanding a RAID Group by Replacing all Disks

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

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

10. Insert a new disk into the same bay.
The NAS beeps twice. Then the status of the disk and RAID group change to *Rebuilding*.
11. Wait for rebuilding to finish.

**Warning**

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

The disks status changes back to *Good*.

12. Repeat the previous steps until all disks in the RAID group have been replaced.
The **Expand Capacity** button is enabled after all disks have been replaced and rebuilding has finished.
13. Click **Expand Capacity**.
A confirmation message appears.
14. Click **OK**.
The NAS beeps and the RAID group status changes to *Synchronizing*.

**Warning**

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

The RAID group status changes to *Ready*.

Changing the RAID Type of a RAID Group

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

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

**Tip**

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

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

**Warning**

All data on the selected disks will be deleted.

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

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

Recovering a RAID Group with an Error Status

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

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

**Important**

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

1. Reconnect all disconnected disks.

**Important**

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

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

QTS starts to rebuild the RAID group.

Recovering a RAID Group with a Degraded Status

If one or more disks fail in a RAID group, but the number of disk failures is within the tolerance of the group's RAID type, then the following events occur:

- The statuses of the RAID group and its storage pool change to *Degraded*.
 - Data on the RAID group and affected storage pool remains accessible.
1. Ensure you have one or more free disks in the NAS.
 2. Go to **Storage & Snapshots > Storage > Storage/Snapshots**.

3. Select a storage pool or single static volume with the status `Degraded`.
4. Click **Manage**.
The **Storage Pool Management** or **Volume Management** window opens.
5. Select a RAID group with the status `Degraded`.
6. Click **Manage**, and then select **Rebuild RAID Group**.
The **Rebuild RAID Group** window opens.
7. Click **Rebuild**.
8. Select one or more disks.
QTS displays the number of disks that you must select, according to the number of disk failures.
9. Click **Apply**.

QTS starts to rebuild the RAID group.

RAID Scrubbing

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



Tip

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

Running RAID Scrubbing Manually



Warning

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

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

The RAID group status changes to `Scrubbing`.

Running RAID Scrubbing on a Schedule


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



Warning

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

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

2. Click the **Global Settings** icon . The **Global Settings** menu opens.
3. Enable **RAID Scrubbing Schedule**.
4. Specify how often data scrubbing will run.
 - Daily
 - Weekly
 - Monthly
5. Specify when data scrubbing will run.


Tip

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

6. Click **Apply**.

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

Self-Encrypting Drives (SEDs)

A self-encrypting drive (SED) is a drive with encryption hardware built into the drive controller. 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 volumes or storage pools | Click New Storage Pool . |
| One or more volumes or storage pools | Click Create , and then select New Storage Pool . |

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

3. 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.

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

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

**Tip**

Use the default RAID type if you are unsure of which option to choose.

For details, see [RAID Types](#).

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

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

For RAID 50 or RAID 60, a spare disk must be configured later. You should configure a global spare disk so that all subgroups share the same spare disk.

9. Optional: Select the number of RAID 50 or RAID 60 subgroups.

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

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

**Warning**

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

10. Click **Next.****11. Optional: Configure SSD over-provisioning.**

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

**Tip**

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

12. Optional: Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
13. 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.

14. Optional: Save the encryption key to the local NAS
Saving the encryption key enables QTS 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.

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

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

Creating an SED Secure Static Volume

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

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

The **Volume Creation Wizard** window opens.

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

**Important**


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

6. Select Create SED secure static volume.

The list of disks only displays SED disks.

7. Select one or more disks.**8. Select a RAID type.**

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

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

**Tip**

Use the default RAID type if you are unsure of which option to choose.

For details, see [RAID Types](#).

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

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

For details, see [RAID Disk Failure Protection](#).

10. Optional: Select the number of RAID 50 or RAID 60 subgroups.

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

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

**Warning**

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

11. Click Next.**12. Optional: Specify an alias for the volume.**

The alias must consist of 1 to 64 characters from any of the following groups:

- Letters: A to Z, a to z
- Special characters: Hyphen (-), underscore (_)

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



Tip

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

14. 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.

15. Specify the SED password.



Warning

Remember this password. If you forget the password, the pool will become inaccessible and all data will be unrecoverable.

16. Optional: Save the encryption key to the local NAS
 Saving the encryption key enables QTS 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.

17. Optional: Configure advanced settings.

| Setting | Description | User Actions |
|---------------------------------------|---|---|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |
| Accelerate performance with SSD cache | QTS adds data from this volume to the SSD cache to improve read or write performance. | No actions |
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | <ul style="list-style-type: none"> • Specify a folder name. • Select Create this folder as a snapshot shared folder. <p>A snapshot shared folder enables faster snapshot creation and restoration.</p> |

18. Click Next.

19. Click Finish.
 A confirmation message appears.



**Warning**

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

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

SED Storage Pool and Static Volume Actions

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

| Action | Description |
|--|---|
| Change SED Pool Password Change SED Volume 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 QTS 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 or volume. All volumes, LUNs, snapshots, and data will become inaccessible until it is unlocked. |
| Unlock | Unlock a locked SED pool or volume. All volumes, LUNs, snapshots, and data will become accessible. |
| Disable SED Security | Remove user password and disable the ability to lock and unlock the volume or pool. |
| Enable SED Security | Add user password and enable the ability to lock and unlock the volume or pool. |

Removing a Locked SED Storage Pool or Static Volume

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

| Option | Description |
|--|--|
| Enter the password of the pool Enter the password of the volume | QTS unlocks the SED disks in the storage pool or static volume, and then deletes all data. |

| Option | Description |
|-----------------|--|
| Forget password | <p>QTS removes the storage pool or static volume without unlocking the disks. The SED disks cannot be used again until you perform one of the following actions:</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**.

SED Erase

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

Erasing a Disk Using SED Erase

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



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

5. Click **Apply**.

Expansion Units

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



Tip
Expansion units used to be known as JBODs.

Expansion Unit Actions

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

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

| Action | Description |
|-------------------------------------|--|
| Action > Rename Enclosure | Rename the selected expansion unit. |
| RAID Group | View details about each RAID group on the expansion unit, including its RAID type, capacity, and member disks. |

Expansion Unit Automatic Recovery



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

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

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

Expansion Unit Recovery

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 than 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 volumes, 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 |

| Device Type | Summary | Example Models |
|---------------|---|-------------------------------|
| Drive Adapter | A small enclosure featuring hardware RAID that allows you to install 1-2 smaller drives into a larger drive bay in a NAS or computer (e.g. two 2.5-inch SATA drives in a 3.5-inch bay). | QDA-A2AR, QDA-A2MAR, QDA-U2MP |

**Note**

When an external RAID enclosure is connected to a QNAP NAS, you can only create one RAID group on the enclosure. All disks not in the RAID group are automatically assigned as spare disks, and cannot be used for storage until the RAID group has been deleted.

Storage Modes

QNAP RAID enclosures support two different storage modes.

**Important**

QNAP drive adapters only support NAS storage mode.

| Storage Mode | Description | Supported RAID Types | Supported Hosts |
|------------------|--|---|--|
| NAS Storage | Use the RAID enclosure's storage capacity to create a new storage pool or static volume on a QNAP NAS. | <ul style="list-style-type: none"> • JBOD • RAID 0 • RAID 1 • RAID 5 • RAID 10 | QNAP NAS running QTS 4.3.6 or later |
| External Storage | Use the RAID enclosure as an external USB disk. This mode supports multiple RAID groups. Each RAID group appears as a separate disk when the enclosure is connected to a host. | <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.
QTS displays all available RAID types and automatically selects the most optimized RAID type.

| Number of disks | Supported RAID Types | Default RAID Type |
|-----------------|-------------------------------|-------------------|
| Two | JBOD, RAID 0, RAID 1 | RAID 1 |
| Three | JBOD, RAID 0, RAID 5 | RAID 5 |
| Four | JBOD, RAID 0, RAID 5, RAID 10 | RAID 5 |



Tip

Use the default RAID type if you are unsure of which option to select.

7. Click **Next**.
8. Select **Create Storage Pool**.
9. Click **Create**.
A confirmation message appears.
10. Click **OK**.
 - The RAID enclosure creates the RAID group.
 - The **Create Storage Pool Wizard** opens on the **Select Disks** screen.
 - The RAID group you created is automatically selected and the RAID type is set to `Single`.
11. Click **Next**.
12. Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
13. Click **Next**.
14. Click **Create**.
A confirmation message appears.
15. Click **OK**.

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

Creating a Storage Pool on a Drive Adapter

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

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

5. Click **Next**.
6. Under **Enclosure Unit**, select **NAS Host**.
7. In the list of disks, select the drive adapter.
8. Under **RAID Type**, select **Single**.
9. Click **Next**.
10. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.



Tip

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

11. Optional: Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
12. Click **Next**.
13. Click **OK**.
 - The **Create Storage Pool Wizard** opens on the **Select Disks** screen.
 - The RAID group created in steps 3-5 is selected as the disk for the storage pool.
 - The RAID type is set to `Single`.
14. Click **Next**.
15. Configure the alert threshold.
QTS issues a warning notification when the percentage of used pool space is equal to or above the specified threshold.
16. Click **Next**.
17. Click **Create**.
A confirmation message appears.

18. Click **OK**.

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

Creating a Static Volume on a RAID Enclosure



Important

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



Warning

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

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



Warning

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

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

| Number of disks | Supported RAID Types | Default RAID Type |
|-----------------|-------------------------------|-------------------|
| Two | JBOD, RAID 0, RAID 1 | RAID 1 |
| Three | JBOD, RAID 0, RAID 5 | RAID 5 |
| Four | JBOD, RAID 0, RAID 5, RAID 10 | RAID 5 |



Tip

Use the default RAID type if you are unsure of which option to select. For details on RAID types, see [RAID Types](#).

7. Click **Next**.
8. Select **Create Volume**.
9. Click **Create**.
A confirmation message appears.
10. Click **OK**.

- The RAID enclosure creates the RAID group.
- The **Volume Creation Wizard** opens on the **Select Disks** screen.
- The RAID group you created is automatically selected and the RAID type is set to `Single`.

11. Click **Next**.

12. Optional: Specify an alias for the volume.


The alias must consist of 1 to 64 characters from any of the following groups:

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

13. Specify the number of bytes per inode.

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

14. Optional: Configure advanced settings.

| Setting | Description | User Actions |
|-----------------|--|--|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |
| Encryption | QTS encrypts all data on the volume with 256-bit AES encryption. | <p>a. Specify an encryption password containing 8 to 32 characters, with any combination of letters, numbers and special characters. Spaces are not allowed.</p> <p>b. Select Save encryption key to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.</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. |

| Setting | Description | User Actions |
|---------------------------------------|---|--|
| Accelerate performance with SSD cache | QTS adds data from this volume to the SSD cache to improve read or write performance. | No actions |
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | <ol style="list-style-type: none"> a. Specify a folder name. b. Select Create this folder as a snapshot shared folder. A snapshot shared folder enables faster snapshot creation and restoration. |

15. Click **Next**.

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

17. Click **OK**.

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

Creating a Static Volume on a Drive Adapter

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

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

The **Volume Creation Wizard** window opens.

5. Select **Static Volume**.
6. Click **Next**.
7. Under **Enclosure Unit**, select **NAS Host**.
8. In the list of disks, select the drive adapter.
9. Under **RAID Type**, select **Single**.
10. Click **Next**.
11. Optional: Specify an alias for the volume.
The alias must consist of 1 to 64 characters from any of the following groups:
 - Letters: A to Z, a to z

- Numbers: 0 to 9
- Special characters: Hyphen (-), underscore (_)

12. Optional: Configure SSD over-provisioning.

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




Tip

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

13. 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.

14. Optional: Configure advanced settings.

| Setting | Description | User Actions |
|---------------------------------------|--|--|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |
| Encryption | QTS encrypts all data on the volume with 256-bit AES encryption. | <p>a. Specify an encryption password containing 8 to 32 characters, with any combination of letters, numbers and special characters. Spaces are not allowed.</p> <p>b. Select Save encryption key to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.</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. |
| Accelerate performance with SSD cache | QTS adds data from this volume to the SSD cache to improve read or write performance. | No actions |

| Setting | Description | User Actions |
|--------------------------------------|---|--|
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | <ol style="list-style-type: none"> a. Specify a folder name. b. Select Create this folder as a snapshot shared folder. A snapshot shared folder enables faster snapshot creation and restoration. |

15. Click **Next**.

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

17. Click **OK**.

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

Configuring a RAID Enclosure as an External Storage Device



Important

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



Warning

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

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



Warning

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

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

| Number of disks | Supported RAID Types | Default RAID Type |
|-----------------|----------------------|-------------------|
| Two | JBOD, RAID 0, RAID 1 | RAID 1 |
| Three | JBOD, RAID 0, RAID 5 | RAID 5 |

| Number of disks | Supported RAID Types | Default RAID Type |
|-----------------|-------------------------------|-------------------|
| 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 <ul style="list-style-type: none"> • Using exFAT on QTS requires an exFAT driver license. You can purchase the license in License Center. • Verify that your device is compatible with exFAT before selecting this option. |
| EXT3 | Linux, NAS devices |
| EXT4 | Linux, NAS devices |

15. Specify a disk label.
The label must consist of 1 to 16 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Hyphen "-"

16. Optional: Enable encryption.**a. Select an encryption type.**

Select one of the following options:

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

b. Specify an encryption password.

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

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

c. Confirm the encryption password.**d. Optional: Select **Save encryption key**.**

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

**Warning**

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

17. Click **Format.**

A warning message appears.

18. Click **OK.**

QTS formats the RAID group on the external RAID enclosure as an external disk. You can view and manage it at **Storage & Snapshots > Storage > External Storage** .







QTS External RAID Management

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

**Warning**

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

| UI Element | Description |
|--------------------------------|---------------------------------|
| External storage device | Select a RAID device to manage. |

| UI Element | Description |
|---|---|
| Safely Detach | <p>Disconnect a RAID device from the NAS when the device is in NAS Storage mode. QTS 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 QTS.</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 or static volume from a QNAP NAS to a different QNAP NAS (which we will call the target NAS).

1. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
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**.
QTS scans the RAID enclosure for storage pools and static volumes, and then displays them on the **Recover Wizard** window.
10. Click **Apply**.

QTS makes all storage pools, volumes, and LUNs on the RAID enclosure available on the target NAS at **Storage & Snapshots > Storage > Storage/Snapshots** .

Manually Updating External RAID Device Firmware in QTS

1. Open **Storage & Snapshots**.
2. Click **External Storage Devices** and then select **External Storage Device Management**.
The **External Storage Device Management** window opens.
3. Select a RAID device.
4. Click **Check for Update**.
The **Firmware Management** window opens. QTS checks online for the latest device firmware.
5. Select a firmware update method.

| Firmware Update Method | Description |
|-------------------------------------|---|
| Install the latest firmware version | Download and install the latest version of the device firmware.  Note You can only select this option if QTS has checked online and found a newer firmware version than the one currently installed on the device. |
| Select a local firmware file | Update the firmware using a local firmware IMG file on your computer. Click Browse to select the file.  Tip You can download firmware updates at https://download.qnap.com . |

6. Click **Update**.

**Warning**

Do not power off or disconnect the RAID device unless prompted.

7. Follow the instructions to install the firmware update.
Depending on the model you may be asked to power off then power on the device, or disconnect then reconnect the device.
QTS re-detects the device and displays a notification message.
8. Wait for confirmation that the firmware update has finished.
9. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
10. Click **Recover**, and then select **Attach and Recover Storage Pool**.

Configuring a Spare Disk

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

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

External RAID Device Health**RAID Enclosure Health**

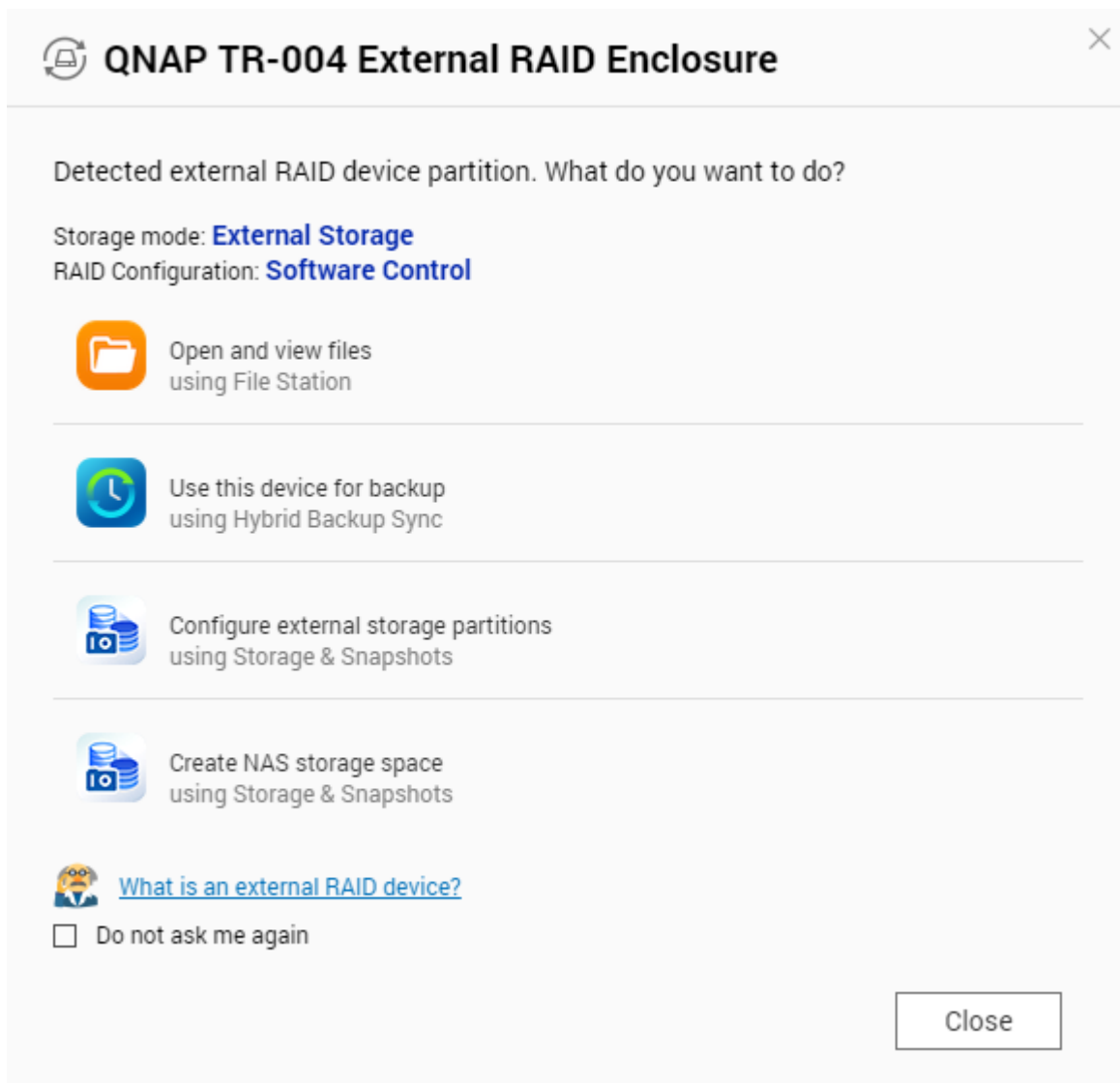
To view the status and health of RAID enclosures connected to the NAS, go to **Storage & Snapshots > Storage > Disks/VJBOD** .

Drive Adapter Health

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

The Autoplay Menu

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



| Action | Description |
|---------------------------------------|---|
| Open and view files | Opens the enclosure in File Station . |
| Use this device for backup | Opens HBS . |
| Configure external storage partitions | Opens Storage & Snapshots > Storage > External Storage . For more information, see Configuring a RAID Enclosure as an External Storage Device . |
| Create NAS storage space | Opens Storage & Snapshots > Storage > Storage/Snapshots . For more information, see: <ul style="list-style-type: none"> 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 or computer. 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 or computer. 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"> • QTS • QuTS hero | <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"> • QTS • QuTS hero | <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"> • QTS • QuTS hero | <ul style="list-style-type: none"> • TL-D800C • TL-R1200C-RP |

QTS JBOD Management

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

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

Updating JBOD Enclosure Firmware in QTS



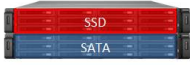

1. Open **Storage & Snapshots**.
QTS periodically checks for the latest firmware for each connected enclosure on login. If a new firmware update is available, QTS opens the **Start Firmware Update** window.
2. Follow the instructions to install the firmware update.
Depending on the model you may be asked to power off then power on the device, or disconnect then reconnect the device.
QTS re-detects the device and displays a notification message.
3. Wait for confirmation that the firmware update has finished.
4. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
5. Click **Recover**, and then select **Attach and Recover Storage Pool**.

Qtier

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

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

Qtier Benefits

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

Qtier 2.0 IO Aware

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

Qtier and SSD Cache Comparison



Note

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

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

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

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

| | Qtier Storage Pool | SSD Cache | All-SSD Storage Pool |
|--------------------------|---|--|--|
| Total file storage space | High (SSDs + HDDs) | Moderate (HDDs only) | Low (SSDs only) |
| Maximum SSD capacity | No limit | Up to 4 TB depending on installed memory | No limit |
| SSD expansion | Expand as needed | Limited by available memory | Expand as needed |
| Applicable storage | Thick volumes, thin volumes and block-based LUNs in the pool | All volumes and LUNs on the NAS | Volumes and LUNs created on the SSDs |
| Data migration | Scheduled or when NAS load is low | Automatic | No migration required |
| Data migration method | QTS writes incoming data to the SSD tier and moves data to different tiers based on access frequency. | <ul style="list-style-type: none"> Write cache: QTS writes incoming data to the SSD cache and then flushes the cache to disk periodically. Read cache: QTS copies data to the cache as it is accessed. | No migration required |
| Recommended use cases | <ul style="list-style-type: none"> Total SSD capacity is high I/O is predictable The storage pool only occasionally experiences periods of intense random I/O access | <ul style="list-style-type: none"> I/O is unpredictable and frequently happens in random bursts Home usage, where the NAS will be used for a large range of different applications | Applications require consistent intensive random read-write access |
| Usage examples | File server, web server, email servers, basic database services (With Qtier IO Aware) | Video editing, virtualization | Business critical database or other application |

Qtier Requirements

NAS Requirements

- The NAS must support Qtier. For a full list of compatible models, see <https://www.qnap.com/solution/qtier-auto-tiering>.
- The NAS should have at least 4 GB of installed memory. Using Qtier with less than 4 GB of memory may cause system instability.

Tier Requirements

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



Important

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

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

Disk Requirements

Qtier Disk Types

| Tier | Disk Type |
|------------------|--|
| Ultra-High Speed | <ul style="list-style-type: none"> • SATA 2.5" SSD • SAS 2.5" SSD • SATA M.2 SSD • PCIe/NVMe M.2 SSD |
| High Speed | <ul style="list-style-type: none"> • SAS HDD |
| Capacity | <ul style="list-style-type: none"> • SATA HDD • NL-SAS HDD |

Qtier Creation

Creating a Qtier Storage Pool

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



Tip


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

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

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

The **Create Storage Pool Wizard** opens.



3. Select **Enable Qtier (auto-tiering storage)**.
4. Click **Next**.
5. Create the ultra-high speed tier.

- a. Click .
- b. Optional: Select an expansion unit.



Important

If you create the ultra-high speed tier using disks installed in a TL-series expansion unit, then the two tiers (high speed, capacity) must consist of disks from the same expansion unit.

- c. Select one or more solid-state drives (SSDs).
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the ultra-high speed tier.
6. Optional: Create the high speed tier.
At least two different tiers are required in a Qtier storage pool.
 - a. Click .
 - b. Optional: Select an expansion unit.
 - c. Select one or more SAS hard disk drives (HDDs).
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the high speed tier.
 7. Optional: Create the capacity tier.
At least two different tiers are required in a Qtier storage pool.
 - a. Click .
 - b. Optional: Select an expansion unit.
 - c. Select one or more SATA or NL-SAS HDDs.
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the capacity tier.
 8. Click **Next**.
 9. Optional: Configure SSD over-provisioning.

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



Tip

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

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



Warning

All data on the selected disks will be deleted.

14. Click **OK**.

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

Enabling Qtier in an Existing Storage Pool

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

1. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select **Qtier > Upgrade with Qtier** .
The **Upgrade Pool to use Qtier Wizard** window opens.
3. Select a storage pool.
4. Click **Next**.
5. Create a second tier.
 - a. Click **SSD** , **SAS** or **SATA** .
 - b. Select an expansion unit.
 - c. Select one or more disks.
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the tier.
6. Optional: Create a third tier.
 - a. Click **SSD** , **SAS** or **SATA** .

- b. Optional: Select an expansion unit.
 - c. Select one or more disks.
 - d. Select a RAID type.
For details, see [RAID Types](#).
 - e. Optional: Select the disk that will be used as a hot spare for the tier.
7. Click **Next**.
 8. Optional: Configure SSD over-provisioning.
Over-provisioning reserves a percentage of SSD storage space on each disk in the RAID group to improve write performance and extend the disk's lifespan. You can decrease the amount of space reserved for over-provisioning after QTS has created the RAID group.

**Tip**

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

9. Click **Next**.
10. Verify the storage pool information.
11. Click **Finish**.
A confirmation message appears.

**Warning**

All data on the selected disks will be deleted.

12. Click **OK**.

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

Qtier Management

Storage Pool 1 Management

+ ×

Qtier Auto Tiering
Storage Pool

Tiering Schedule
Tiering On Demand
Statistics

Qtier Auto-Tiering Status of Storage Pool 1

Tiering Status: Idle

Schedule Setting: Automatic data tiering

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

| Tier | Used | Total | Move Down | Move Up | Name/Alias | RAID Type |
|-------------------------|--|-----------|-----------|---------|------------------------------|-------------|
| Tier1: Ultra-High Speed | <div style="width: 33.2%; height: 10px; background: linear-gradient(to right, #007bff, #ccc);"></div> 33.2 % | 204.59 GB | 0 MB | -- | RAID Group 1 | RAID 0(2+0) |
| Tier2: High Speed | -- | -- | 0 MB | 0 MB | -- | -- |
| Tier3: Capacity | <div style="width: 1.0%; height: 10px; background: linear-gradient(to right, #007bff, #ccc);"></div> 1.0 % | 3.62 TB | -- | 0 MB | RAID Group 2 | RAID 0(2+0) |

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

Close

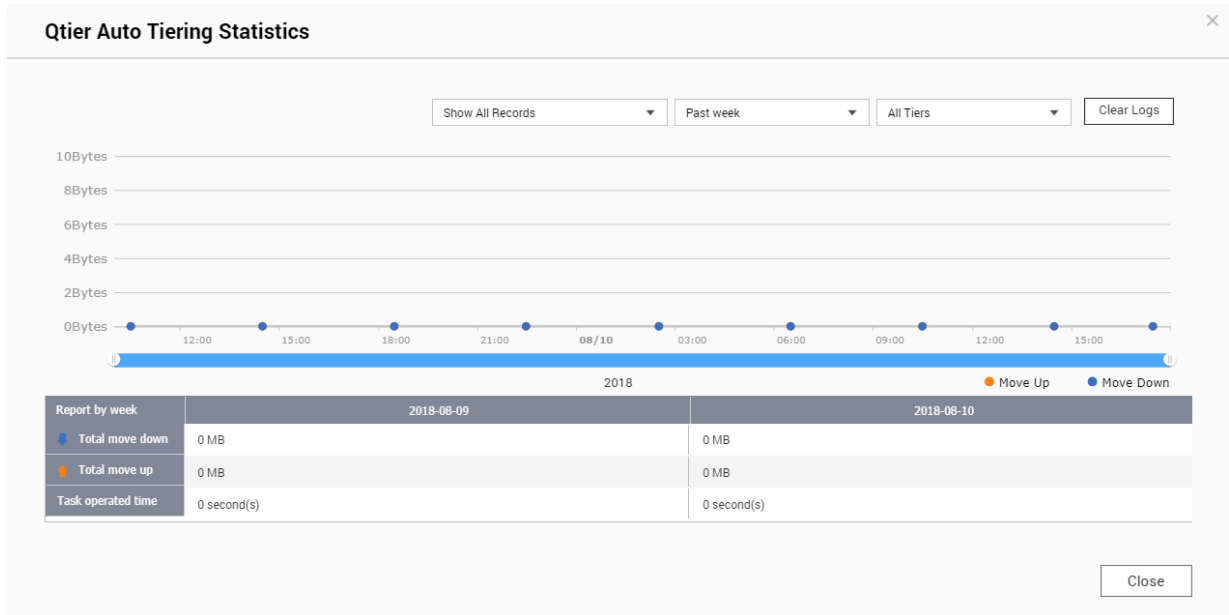
The Qtier Storage Pool Management Screen

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

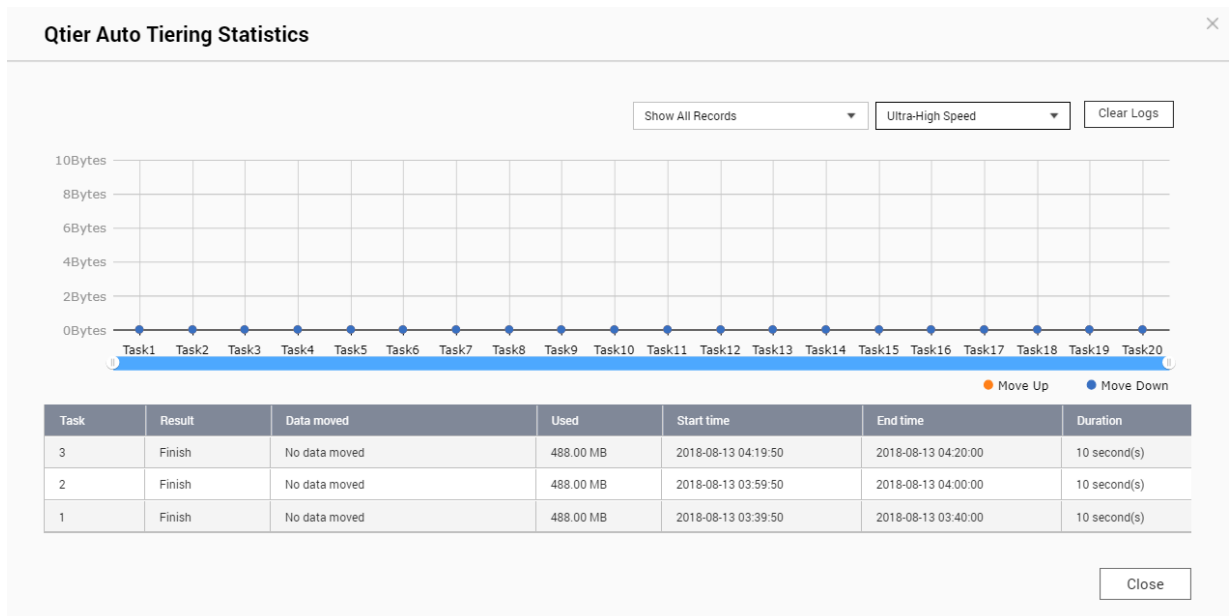
Qtier Statistics

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

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



Qtier Statistics (Automatic data tiering)



Qtier Statistics (Manually set tiering schedule)

Qtier Status

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

Qtier Tiering Schedule

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



Tip

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

Configuring the Qtier Tiering Schedule

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

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

| Option | Description | Recommended usage | User Actions |
|-------------------------------|--|--|---|
| Manually set tiering schedule | Qtier only move data at the times you specify. | The NAS has a regular known usage pattern. For example, if the NAS is primarily used in an office environment, Qtier can be scheduled to move data at night and on weekends. | Specify the hours on the calendar that Qtier should perform data tiering. You can configure the following settings: <ul style="list-style-type: none"> • Start minutes: Auto tiering will start at this number of minutes past the hour. • Run now: Start tiering data immediately. |

7. Click **Apply**.

Removing the Ultra-High Speed Tier

Removing the ultra-high speed tier converts a Qtier storage pool into a regular storage pool.



Important

You can only remove the ultra-high speed tier if the allocated storage pool space is less than the remaining storage pool capacity (Total storage pool capacity - Ultra-high speed tier capacity = Remaining capacity).



Tip

This feature is useful in the following situations:

- You want to use the SSD drives for another purpose.
- You want to increase the amount of SSD over-provisioning in the ultra-high speed tier.
- You want to change the RAID configuration of the ultra-high speed tier.

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

2. Select a Qtier storage pool.

3. Click **Manage**.

The **Storage Pool Management** window opens.

4. Click **Remove** and then select **Remove Ultra-High Speed Tier**.

The **Ultra-High Speed Tier Removal Wizard** window opens.

5. Click **Next**.

6. Confirm that you want to remove the remove ultra-high speed tier.

7. Click **Next**.



Warning

The storage pool will be inaccessible while QTS removes the ultra-high speed tier. This process might take a long time.

8. Click **Finish**.

QTS creates a background task. The status of the storage pool changes to `Removing SSD Tier...`

Tiering On Demand

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



Important

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

Configuring Tiering On Demand

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

Snapshots

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

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



Note

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

Snapshot Storage Limitations

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



Tip

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

| NAS CPU or Model | Installed Memory | Maximum Snapshots per NAS | Maximum Snapshots per Volume or LUN |
|--------------------------|------------------|---------------------------|-------------------------------------|
| • Intel CPU • AMD CPU | ≥ 1 GB | 32 | 16 |
| | ≥ 2 GB | 64 | 32 |
| | ≥ 4 GB | 1024 | 256 |

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

Snapshot Creation

Taking a Snapshot


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



Tip

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

3. Click **Snapshot** and then select **Take a Snapshot**.
The **Take a Snapshot** window opens.
4. Optional: Specify a name.
5. Optional: Choose to keep the snapshot permanently.
If selected, QTS retains the snapshot indefinitely. If not selected, QTS may delete the snapshot according to the snapshot retention policy set for the volume or LUN.
For more information, see [Snapshot Retention Policy](#).
6. Select the LUN snapshot type.
This setting is only available when taking a snapshot of a block-based LUN.

| Type | Description |
|------------------------|---|
| Crash consistent | The snapshot records the state of the data on the LUN. |
| Application consistent | <p>The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QTS takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot.</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> |

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

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


Configuring a Snapshot Schedule



Tip

You can configure a separate snapshot schedule for each volume and LUN.

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

| Type | Description |
|------------------------|--|
| Crash consistent | The snapshot records the state of the data on the LUN. |
| Application consistent | <p>The snapshot records the state of data and applications on the LUN. The iSCSI host flushes data in memory to the LUN before QTS takes a snapshot. If VMware vCenter is using the LUN, vCenter takes a virtual machine snapshot.</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> |

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

QTS starts taking snapshots according to the schedule.

Snapshot Management

Snapshot Retention Policy

The snapshot retention policy determines how long QTS keeps each snapshot of a volume or LUN before deleting it. Each volume and LUN has its own individual snapshot retention policy.


Configuring a Snapshot Retention Policy



Important

After you create or modify a snapshot retention policy, QTS applies the new policy to existing snapshots. If the new policy is more restrictive than the previous policy, for example changing from `Keep for: 5 days` to `Keep for: 2 days`, then QTS deletes existing snapshots to conform with the new policy.

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

| Snapshot Retention Policy | UI Label | Description |
|---------------------------|--|--|
| Time-based | Keep for | Keep each snapshot for the specified length of time. |
| Fixed number | Keep the specified number of snapshots | Keep a fixed maximum number of snapshots on the NAS. After the maximum number is reached, QTS 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. <p> Important The maximum number of snapshots for all time periods combined is 256.</p> |


7. Click **OK**.

Configuring Pool Guaranteed Snapshot Space

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



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

1. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
2. Select a thick volume, thin volume, or LUN.
3. Click **Snapshot**, and then select **Snapshot Manager**.
4. Click **Pool Guaranteed Snapshot Space**, and then select **Configure**.
5. Enable **Enable Pool Guaranteed Snapshot Space**.
6. Select the amount of reserved space.

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

7. Click **OK**.

Deleting Snapshots

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

Snapshot Data Recovery



Restoring Files and Folders from a Snapshot



Tip

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

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

| Action | Description |
|--|--|
| Select Restore > Restore Files | Restore the files or folders to their original storage location. If the files or folders still exists on the NAS, then they will be overwritten with the older versions.  Warning All changes made after the snapshot was taken will be deleted. |
| Select Restore > Restore Files to | Choose one of the following restoration options. <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. |

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

Reverting a Volume

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

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

**Important**

The volume must have at least one snapshot.

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

**Warning**

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

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

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

Reverting a LUN

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

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

**Important**

The LUN must have at least one snapshot.

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

**Warning**

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

6. Optional: Configure the following settings.

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

7. Click **Local Revert**.

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

Restoring Files and Folders using Windows Previous Versions


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



Important

- You must be using Windows 7, Windows 8 or Windows 10.
- The files must be stored on a thick volume or thin volume that has at least one snapshot.
- **Enable Windows Previous Versions** must be enabled in the shared folder settings.
- **Allow symbolic links between different shared folders** must be enabled at **Control Panel > Network & File Services > Win/Mac/NFS > Microsoft Networking > Advanced Options** .

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

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

Snapshot Clone

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

Cloning a Volume

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



Important

The volume must have at least one snapshot.

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

5. Click **Clone**.
The **Clone Snapshot** window opens.
6. Specify a volume alias.
7. Click **OK**.

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

Cloning a Block-Based LUN

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



Important

The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.
The **Snapshot Manager** window opens.
4. Select a snapshot.
5. Click **Clone**.
The **Clone Snapshot** window opens.
6. Specify a LUN name.
7. Optional: Select an iSCSI target.
QTS will map the LUN copy to the target.
8. Click **OK**.

QTS clones the LUN and then displays a confirmation message.

Snapshot Replica

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

Protection Levels

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

| Protects Against | Snapshots only | Snapshots + Local Snapshot Replica | Snapshots + Remote Snapshot Replica |
|--|----------------|------------------------------------|-------------------------------------|
| Accidental modification or deletion of files | ✓ | ✓ | ✓ |
| Ransomware | ✓ | ✓ | ✓ |

| Protects Against | Snapshots only | Snapshots + Local Snapshot Replica | Snapshots + Remote Snapshot Replica |
|---|----------------|------------------------------------|-------------------------------------|
| 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 • QTS encounters an error and cannot start • NAS is stolen | | | ✓ |

Snapshot Replica Requirements

| NAS | Requirement |
|----------------------------|--|
| Source and Destination NAS | Must be a QNAP NAS that supports snapshots. |
| Source and Destination NAS | Both source and destination NAS devices must be running QTS. Replicating snapshots from QTS to QuTS hero or vice versa is not supported. |
| Source and Destination NAS | Must have at least 1GB of installed memory. |
| Source and Destination NAS | SSH port 22 and TCP data ports 50100-50199 must be open. |
| Destination NAS | The NAS must have at least one storage pool with free space greater than or equal to the size of the volume or LUN being backed up. |
| Destination NAS | Allow SSH connections must be enabled at Control Panel > Network & File Servers > Telnet / SSH . |

Creating a Snapshot Replica Job



Important

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

1. Go to **Storage & Snapshots > Snapshot Backup > Snapshot Replica** .
2. Click **Create a Replication Job**.
The **Create a Snapshot Replication Job** wizard opens.
3. Select the source volume or LUN.

- Optional: Specify a job name.

**Tip**

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

- Click **Next**.
- 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 |

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

**Tip**

The default port is 22.

- Click **Test**.
QTS connects to the destination NAS using the specified admin password, and checks that there is sufficient storage space.
- Click **Next**.
- Specify how many replicated snapshots will be kept on the destination NAS.
After the specified number is reached, QTS will delete the oldest snapshot each time it replicates a new snapshot.
- Select the destination storage pool.
- Click **Next**.
- Select a backup plan.


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

| Backup Plan | Description |
|---|---|
| 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. QTS 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>QTS encrypts the snapshot before replicating it.</p> <ul style="list-style-type: none"> • The job must be run by the NAS admin user • The port used by this job must be the same as the SSH port on the destination NAS |






| Setting | Description |
|------------------------|--|
| Compress transfer | <p>QTS compresses snapshots when replicating them. This consumes more CPU and system memory, but reduces the amount of bandwidth required.</p> <p> Tip Enable this setting in low bandwidth networks, or if the NAS devices are connected through a WAN.</p> |
| Maximum transfer speed | Limits how much network bandwidth this job uses |


17. Optional: Export the source data to an external storage device.
To save time and bandwidth, you can export the source data to a connected external storage device such as a USB disk. After connecting the external storage device to the destination NAS, QTS 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**.
QTS creates the job.
22. Optional: If you chose to export source data to an external storage device, disconnect the storage device from the source NAS and connect it to the destination NAS.

Snapshot Replica Management

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

Snapshot Replica Job Actions

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

| Icon | Description |
|---|-------------|
|  | Delete |

Snapshot Replica Options

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

Data Recovery on a Source NAS

Restoring Files and Folders from a Remote Snapshot



Important

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

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




Important

The volume must be the source volume for a Snapshot Replica job.

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

| Action | Description |
|--|---|
| Select Restore > Restore Files | <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 data-bbox="676 1666 735 1729" data-label="Image"> </div> <div data-bbox="754 1657 873 1693" data-label="Section-Header"> <h4>Warning</h4> </div> <div data-bbox="754 1691 1334 1753" data-label="Text"> <p>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. |

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

Reverting a Volume Using a Remote Snapshot

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



Important

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

- Go to **Storage & Snapshots > Storage > Storage/Snapshots**.
- Select a thick or thin volume.



Important

The volume must be the source volume for a Snapshot Replica job.

- Click **Snapshot**, and then select **Snapshot Manager**.
The **Snapshot Manager** window opens.
- Under **Select snapshot location**, select a remote NAS.
- Select a snapshot.
- Click **Revert Volume Snapshot**.



Warning

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

- Optional: Configure the following settings.

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



Warning

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

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

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

Reverting a LUN Using a Remote Snapshot

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



Warning

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

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



Important

The LUN must have at least one snapshot.

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



Warning

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

7. Optional: Configure the following settings.

| Setting | Description |
|--|---|
| Take a new snapshot before reverting | QTS takes a snapshot before starting the revert. This ensures that changes made to data since the snapshot was taken are not permanently lost. |
| Enable encryption during transfer | QTS encrypts the snapshot before sending it for additional security. |
| Re-map LUN to the same iSCSI target after revert | If enabled, QTS automatically remaps the LUN to its current target after reverting. If disabled, you must manually remap the LUN after reverting. |

**Warning**

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

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

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

Cloning a Volume from a Remote Snapshot**Important**

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

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

**Important**

The volume must have at least one snapshot.

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

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

Cloning a Block-Based LUN from a Remote Snapshot

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

**Important**

The LUN must have at least one snapshot.

3. Click **Snapshot**, and then select **Snapshot Manager**.

The **Snapshot Manager** window opens.

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


QTS clones the LUN and then displays a confirmation message.

Data Recovery on a Destination NAS


Snapshot Vault

After setting a NAS as the destination for a Snapshot Replica job, the replicated snapshots are stored in **Storage & Snapshots > 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 volume is encrypted, you must unlock the vault with the volume's encryption password.
 - a. Click **Unlock**.
 - b. Enter the encryption password or upload the encryption key.
 - c. Click **OK**.
5. Select a snapshot.
6. Select the files and folders to be restored.
7. Click **Restore Files To**.
8. Specify a restore location.
9. Click **OK**.

Cloning a Volume from a Snapshot Vault

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


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

Cloning a Block-Based LUN from a Snapshot Vault



Important

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

1. Go to **Storage & Snapshots > Snapshot Backup > Snapshot Vault** .
2. Select a storage pool.
3. On a vault, click  .
The **Snapshot Vault** window opens.
4. Select a snapshot.
5. Click **Clone**.
The **Clone Snapshot** window opens.
6. Specify a LUN name.
7. Optional: Select an iSCSI target.
QTS will map the LUN copy to the target.
8. Click **OK**.

QTS clones the LUN and then displays a confirmation message.

Cache Acceleration

Cache Acceleration enables you to create an SSD cache to improve the read and write performance of the NAS.

Cache Acceleration Requirements

- The NAS model must support Cache Acceleration.
For information about NAS and drive bay compatibility, see <https://www.qnap.com/solution/ssd-cache>.
- The NAS must have one or more free SSDs installed in a compatible drive bay.
- The NAS must have a suitable amount of installed memory.
The amount of memory required depends on the size of the SSD cache.

| SSD Cache Size | Required Memory |
|----------------|-----------------|
| 512GB | ≧ 1GB |
| 1TB | ≧ 4GB |
| 2TB | ≧ 8GB |
| 4TB | ≧ 16GB |

Creating the SSD Cache

1. Go to **Storage & Snapshots > Storage > Cache Acceleration**.
2. Click .
The **Create SSD Cache** window opens.
3. Click **Next**.
4. Select one or more SSDs.



Warning

All data on the selected disks will be deleted.

5. Select a cache type.

| Cache Type | Description |
|------------|--|
| Read-only | When data is read from a LUN or volume, QTS copies the data to the SSD cache to speed up future read requests. |
| Write-only | QTS writes incoming data to the SSD cache first, then flushes the data to regular storage later. Read access to the new data is also accelerated while it is in the cache. |
| Read-write | QTS uses the SSD cache for both read and write caching, accelerating both read and write speeds. |

6. Select a RAID type.



Warning

Selecting a RAID type with no disk failure protection (Single, JBOD, RAID 0) when the cache type is *Write-only* or *Read-write* may result in data loss.

**Tip**

RAID 10 provides the best write cache performance.

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

**Tip**

To determine the optimal amount of over-provisioning for your SSDs, download and run SSD Profiling Tool from App Center.
For details, see [SSD Profiling Tool](#).

9. Select a cache mode.

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

**Tip**

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

10. Optional: Configure the following advanced settings.

| Setting | Description |
|--------------------------|---|
| Bypass block size | This value determines the maximum size of the data blocks that are stored in the SSD cache. Selecting a larger size may improve the cache's hit rate but uses more cache space. The default value is 1 MB. |
| Cache replacement policy | Specify how data is removed from the SSD cache. Choose one of the following options: <ul style="list-style-type: none"> • Least recently used (LRU): Better cache performance but uses more CPU resources. This is the default option. • First in first out (FIFO): Lower CPU usage than LRU but might cause worse cache performance. |

11. Click **Next**.
12. Select which volumes and LUNs can use the SSD cache.

**Important**

For data safety, volumes and LUNs created on an external storage device cannot use the SSD cache if the cache type is `Read-write`.

13. Click **Next**.
14. Click **Create**.
A confirmation message appears.
15. Select **I understand** and then click **OK**.

Expanding the SSD Cache

The SSD cache can be expanded by adding a new SSD RAID group.



Important

Expanding the SSD cache clears all cached data.

1. Go to **Storage & Snapshots > Storage > Cache Acceleration**.
2. Click **Manage** and then select **Expand**.
A confirmation message appears.
3. Click **OK**.
4. Select one or more SSDs.



Warning

All data on the selected disks will be deleted.

5. Select a RAID type.



Warning

Selecting a RAID type with no disk failure protection (Single, JBOD, RAID 0) when the cache type is `Write-only` or `Read-write` may result in data loss.



Tip

RAID 10 provides the best write cache performance.

6. Click **Expand**.
A confirmation message appears.
7. Click **OK**.

Configuring SSD Cache Settings

1. Go to **Storage & Snapshots > Storage > Cache Acceleration**.
2. Click **Manage** and then select **Settings**.
The **Switch SSD Cache** window opens.
3. Select which volumes and LUNs can use the SSD cache.



Important

For data safety, volumes and LUNs created on an external storage device cannot use the SSD cache if the cache type is `Read-write`.

4. Click **Next**.
5. Select a cache mode.

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

**Tip**

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

- Optional: Configure bypass block size.
This value determines the maximum size of the data blocks that are stored in the SSD cache. Selecting a larger size may improve the cache's hit rate but uses more cache space. The default value is 1 MB.
- Click **Finish**.

Cache Missing

If the write-only or read-write cache disks become unavailable because of hardware failure or physical removal from the NAS, all volumes using the write-cache will also become unavailable and will have `Cache Missing` as their status. QTS restricts access to these volumes to protect data integrity, as some volume data may be stored in the write cache without being flushed to disk.

When the SSD cache is missing, restore it using one of the following methods:

- If the SSD cache disks were removed from the NAS, re-insert the disks into the same drive bays.
- Resolve any RAID errors.
- Restart the NAS.

Removing a Missing SSD Cache

**Important**

You should only delete a missing SSD cache if it is not possible to restore the cache, for example, because of disk failure.

**Warning**

Removing a missing SSD write-only or read-write cache will delete all unflushed write data.

- Go to **Storage & Snapshots > Storage > Cache Acceleration**.
- Select **Manage > Remove**.
A confirmation message appears.
- Enter the admin password.
- Click **OK**.
- Restart the NAS.

- Run a file system check on all volumes that used the SSD cache.
For the details, see [Volume File System Check](#).

Removing the SSD Cache



Warning

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

- Go to **Storage & Snapshots > Storage > Cache Acceleration**.
- Click **Manage** and then select **Remove**.
A confirmation message appears.
- Click **OK**.

QTS flushes all data in the cache to disk, then deleted the RAID groups. This process make take a long time.

External Storage

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



Note

To access partitions formatted using the exFAT file system, you must purchase an exFAT driver license in License Center.

External Storage Device Actions

| Action | Description |
|--------|---|
| Erase | Delete all data and partitions on the device. |
| Eject | Safely unmount the external storage device from the NAS, so that you can disconnect it. |

External Storage Disk Actions

| Action | Description |
|------------------|---|
| Full Disk Format | Format the disk. For details, see Formatting an External Storage Partition . |
| Secure Erase | Permanently erase all data on a disk. For details, see Secure Erase . |



External Storage Partition Actions

| Action | Description |
|---------------------|--|
| Storage Information | Displays details about the selected partition, including partition name, capacity, used space, and file system type. |
| Format | Formats the partition. For details, see Formatting an External Storage Partition . |

| Action | Description |
|-----------------------|---|
| Encryption Management | Manages encryption on a previously encrypted device. You can lock or unlock the device, change the encryption password, or download the encryption key. |
| Eject | Unmounts the partition. The external storage device and any stored partitions will continue working. |

Formatting an External Storage Partition

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

| File System | Recommended Operating Systems and Devices |
|-------------|--|
| NTFS | Windows |
| HTS+ | macOS |
| FAT32 | Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets  Important The maximum file size is 4 GB. |
| exFAT | Windows, macOS, some cameras, mobile phones, video game consoles, tablets  Important <ul style="list-style-type: none"> • Using exFAT on QTS requires an exFAT driver license. You can purchase the license in License Center. • Verify that your device is compatible with exFAT before selecting this option. |
| EXT3 | Linux, NAS devices |
| EXT4 | Linux, NAS devices |

5. Specify a disk label.
The label must consist of 1 to 16 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Hyphen "-"
6. Optional: Enable encryption.
 - a. Select an encryption type.
Select one of the following options:
 - AES 128 bits

- AES 192 bits
 - AES 256 bits
- b. Specify an encryption password.
The password must consist of 8 to 16 characters from any of the following groups:
- Letters: A to Z, a to z
 - Numbers: 0 to 9
 - All special characters (excluding spaces)
- c. Confirm the encryption password.
- d. Optional: Select **Save encryption key**.
Select this option to save a local copy of the encryption key on the NAS. This enables QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts.



Warning

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

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

Remote Disk

Remote disk enables QTS to act as an iSCSI initiator, allowing you to expand NAS storage by adding iSCSI LUNs from other NAS or storage servers as remote disks. When connected, remote disks are automatically shared on the **Shared Folders** screen. If a remote disk is disconnected, the disk will become inaccessible and QTS will try to reconnect to the target after 2 minutes. If the target cannot be reached, the status of the remote disk will change to *Disconnected*.

This feature is only available on NAS models that support iSCSI.

Remote Disk Limitations

| Limit | Value |
|--|-------------------------------|
| Maximum number of remote disks per NAS | 8 |
| Supported file systems | ext3, ext4, FAT32, NTFS, HFS+ |
| Maximum remote disk size | 16 TB |

Adding a Remote Disk

1. Go to **Storage & Snapshots > Remote Disk**.
2. Click **Add Virtual Disk**.


3. Specify the IP address or hostname of the remote server.
4. Optional: Specify the iSCSI port of the remote server.
5. Click **Get Remote Disk**.
QTS connects to the remote server and then lists all available iSCSI targets.
6. Select an iSCSI target.
7. Optional: Specify a CHAP username and password.
This is required if the remote server has CHAP authentication enabled.
8. Optional: Enable CRC checksums.
Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

| Checksum Type | Description |
|---------------|---|
| Data Digest | The checksum can be used to verify the data portion of the PDU. |
| Header Digest | The checksum can be used to verify the header portion of the PDU. |

9. Click **Next**.
10. Optional: Specify a disk name.
The name must consist of 1 to 50 characters from the following groups:
 - Letters: a to z, A to Z
 - Numbers: 0-9
 - Special characters: space (), hyphen (-), underscore (_), period (.)

The following are not allowed:

 - The last character is a space
 - The name starts with "_sn_"
11. Select a LUN.
12. Optional: Format the disk.
Select one of the following options.

| File System | Compatible Operating Systems and Devices |
|-------------|--|
| ext4 | Linux, NAS devices |
| ext3 | Linux, NAS devices |
| FAT32 | Windows, macOS, NAS devices, most cameras, mobile phones, video game consoles, tablets  Important The maximum file size is 4 GB. |
| NTFS | Windows |
| HTS+ | macOS |

**Warning**

All data on the LUN will be deleted.

13. Configure synchronous I/O.

If the remote server is using ZFS, select the ZFS Intent Log I/O mode for the LUN to improve data consistency or performance.

| Mode | Description |
|--------------|---|
| Synchronous | All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a small impact on performance. |
| Asynchronous | All I/O transactions are treated as asynchronous. This option gives the highest performance, but has a higher risk of data loss in the event of a power outage. Ensure that a UPS (uninterrupted power supply) is installed when using this option. |

14. Click Next.**15. Click Finish.**

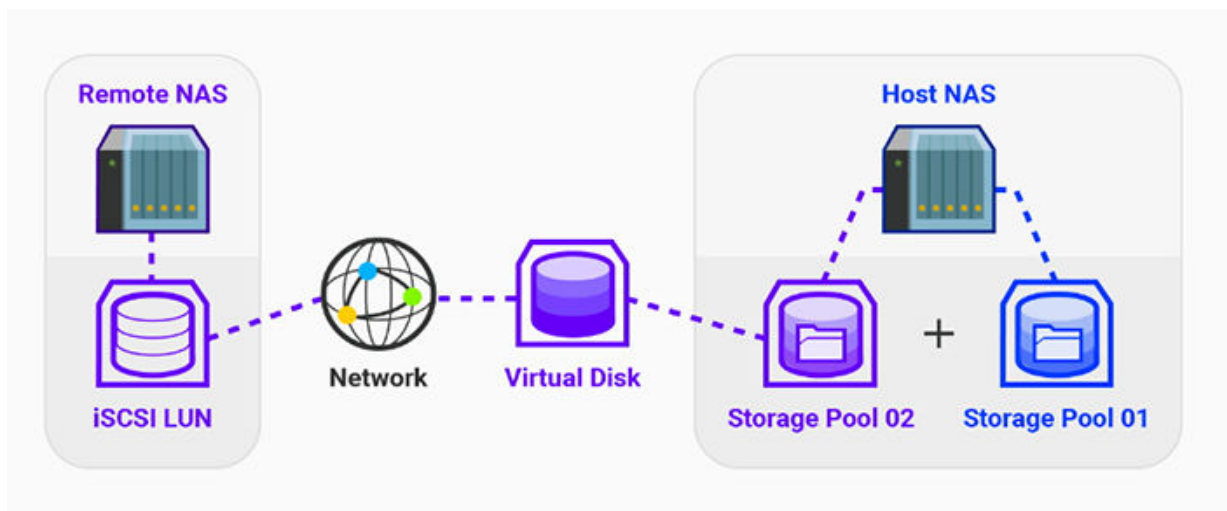
QTS adds the remote disk and shares it at **Control Panel > Privilege > Shared Folders** . By default only the admin account has access.

Remote Disk Actions

| Action | Description |
|--------|--|
| Edit | Edit the name of the disk. |
| Delete | Disconnect the remote disk and delete its shared folder. Existing data on the disk will not be deleted. |
| Format | Format the remote disk. Select one of the following file system options: <ul style="list-style-type: none"> • ext4 • ext3 • FAT32 • NTFS • HTS+ Select one of the following I/O options: <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.
- It is not possible to create a system volume using VJBOD disks.
- VJBOD disks only support the RAID type Single.

VJBOD Automatic Reconnection

If a remote NAS gets disconnected, QTS automatically tries to reconnect to the NAS and recover the VJBOD disk every 30 seconds.



Important

- To allow automatic reconnection, all NAS devices should be configured with static IP addresses.
- The following things may prevent VJBOD connection or reconnection:
 - Use of dynamic IP addresses
 - Host IQN binding
 - Firewalls of IP blocks
 - Incorrect CHAP credentials

VJBOD Creation

Creating a VJBOD Disk from a New LUN

1. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
2. Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.
3. Click **Next**.
4. Specify the IP address or hostname of the remote NAS.



Important

The remote NAS must have at least one storage pool containing at least 153 GB of free space.



Tip

Click **Detect** to view the IP addresses of all QNAP NAS devices on the local network. Click **Local Host** to use the IP of the local NAS.

5. Specify the admin password of the remote NAS.
6. Optional: Specify the system administration port of the remote NAS.



Tip

The default port is 8080, or 443 if HTTPS is enabled.

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 |
|----------------------|--|
| 4K bytes sector size | Changing the sector size to 4 KB increases LUN performance for specific applications and disk types. |
| SSD cache | The SSD cache will be used to improve VJBOD disk access performance. |

19. Click **Next**.
QTS 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 128 characters
 - Valid Characters: 0 to 9, a to z, A to Z
 - Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z
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**.

QTS creates the iSCSI target and LUN on the remote NAS, and then creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots > Storage > Disks/VJBOD** .

24. Select a follow-up action.

| Action | Description |
|--------------------------|--|
| Create New Storage Pool | Creates a storage pool using the VJBOD disk |
| Create New Static Volume | Creates a static volume using the VJBOD disk |
| Do nothing | Ends the creation process. You can configure the VJBOD disk later. <div style="display: flex; align-items: flex-start;">  <div> <p>Tip To create a storage pool or static volume on a VJBOD disk later, go through the normal steps of creating a storage pool or static volume. Then on the disk selection screen, under Enclosure Unit select <code>Virtual JBOD</code>.</p> </div> </div> |

25. Click **Finish**.

Creating a VJBOD Disk from an Existing LUN

- Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
- Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.
- Click **Next**.
- 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.

- Specify the admin password of the remote NAS.
- Optional: Specify the system administration port of the remote NAS.



Tip

The default port is 8080, or 443 if HTTPS is enabled.

- 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 128 characters
 - Valid Characters: 0 to 9, a to z, A to Z
 - Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z
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**.
QTS 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 |
| Create New Static Volume | Creates a static volume using the VJBOD disk |
| Recover Existing Data | Restores a static volume or storage pool that was previously created on the VJBOD disk |
| Do nothing | <p>Ends the creation process. You can configure the VJBOD disk later.</p> <p> Tip To create a storage pool or static volume on a VJBOD disk later, go through the normal steps of creating a storage pool or static volume. Then on the disk selection screen, under Enclosure Unit select Virtual JBOD.</p> |

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/VJBOD Cloud**, and then select **VJBOD Overview**.

| Virtual JBOD Overview | | | | | | | | | |
|--|--------|------------|--------------------------------------|------------------|----------------------------|--|----------------------------------|---------------------|-----------------|
| 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:tsca1: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:tsca1: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 |
|---------------|-------------|--|
| New Volume | Free | Creates a new static volume on the VJBOD disk |
| NAS Detail | Any | Displays information about VJBOD disk's remote NAS |
| Remote Log | Any | Displays the event log on the VJBOD disk's remote NAS |
| Data Recovery | Free | Restores a static volume or storage pool that was previously created on the VJBOD disk |

| Action | Disk Status | Description |
|-------------|--------------|---|
| 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 or static volume. You can then connect the LUN to another NAS, create a new VJBOD disk, and recover the pool or volume using Action > Data Recovery . |
| Delete | Disconnected | Deletes a VJBOD from the local disk. The LUN and all data will remain on the remote NAS. You can also choose to delete the iSCSI target and LUN on the remote NAS. |

Moving a VJBOD Disk to Another QNAP NAS

1. Note the details of the VJBOD disk's remote LUN.
 - a. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
 - b. Click **VJBOD/VJBOD Cloud**, and then select **VJBOD Overview**.
The **VJBOD Overview** window opens.
 - c. Locate the VJBOD disk that you want to move, and then note the **Remote LUN Name** and the IP address under **Remote NAS**.
2. Detach the VJBOD disk's static volume or storage pool.
 - a. Go to **Storage & Snapshots > Storage > Storage/Snapshots** .
 - b. Select the static volume or storage pool on the VJBOD disk.
 - c. Click **Manage**.
The **Volume Management** or **Storage Pool Management** window opens.
 - d. Click **Action**, and then select **Safely Detach**.
3. Remove the VJBOD disk from the NAS.
 - a. Go to **Storage & Snapshots > Storage > Disks/VJBOD** .
 - b. Select the VJBOD disk.
 - c. Click **Action**, and then select **Disconnect**.
The status of the VJBOD disk changes to *Disconnected*.
 - d. Click **Action**, and then select **Delete**.
QTS removes the VJBOD disk from the local NAS.
4. Add the VJBOD disk on another QNAP NAS.
 - a. On the other NAS, go to **Storage & Snapshots > Storage > Disks/VJBOD** .

- b. Click **Create**, and then select **Create Virtual JBOD**.
The **Create Virtual JBOD Disk Wizard** opens.
- a. Click **Next**.
- b. Specify the IP address or hostname of the remote NAS.
- c. Specify the admin password of the remote NAS.
- d. Optional: Specify the system administration port of the remote NAS.

**Tip**

The default port is 8080, or 443 if HTTPS is enabled.

- e. Click **Next**.
- f. Optional: Select the local interface that will be used by VJBOD.
- g. Optional: Select the remote interface that will be used by VJBOD.
- h. Optional: Select **Use iSER when available**.
Enabling iSER increases data transfer speeds and reduces CPU and memory load.
- i. Click **Next**.
- j. Select **Choose an existing iSCSI LUN on the selected NAS**.
- k. Click **Next**.
- l. Select the LUN containing the VJBOD disk.
- m. Click **Next**.
- n. 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. |

- o. Click **Next**.
- p. Review the summary, and then click **Next**.
QTS creates a VJBOD disk using the LUN. The disk appears at **Storage & Snapshots > Storage > Disks/VJBOD**.
- q. In the actions list, select **Recover Existing Data**.
- r. Click **Finish**.

QTS scans for and restores any storage pools, volumes, and LUNs on the VJBOD disk.

VJBOD Cloud

VJBOD Cloud is a block-based storage gateway solution that enables you to create volumes and LUNs on your NAS using cloud space from cloud services such as Google Cloud and Amazon S3. VJBOD Cloud volumes and LUNs can utilize local storage space for accelerated read and write speeds, allowing both NAS users and applications to seamlessly and transparently access cloud storage space.


Installation

VJBOD Cloud Requirements

Requirements:

- A QNAP NAS running QTS 4.4.1 or later
- A cloud space (bucket or container) with at least 1 GB of free space from a supported cloud service provider

Installing VJBOD Cloud

1. Log on to QTS as administrator.
2. Ensure that a system volume is configured on the NAS.
For details, see [The System Volume](#).
3. Open **App Center**, and then click .
A search box appears.
4. Type `VJBOD Cloud`, and then press `ENTER`.
The VJBOD Cloud application appears in the search results.
5. Click **Install**.
The installation window appears.
6. Select the volume on which you want to install VJBOD Cloud.
7. Click **OK**.
QTS installs VJBOD Cloud.

VJBOD Cloud Volume and LUN Creation

Creating a VJBOD Cloud Volume

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

6. Optional: Select **Use system proxy settings.**

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

7. Click **Search.****8. Select a cloud space.**

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

**Note**

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

9. Optional: Click **Performance test.**

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

10. Click **Next.****11. Select **Create a new volume**.****12. Optional: Specify an alias for the volume.**

Alias requirements:

- Length: 1–64 characters
- Valid characters: A–Z, a–z, 0–9
- Valid special characters: Hyphen (-), Underscore (_)

13. Specify the capacity of the volume.


The amount of free space in the cloud storage space determines the maximum capacity.

**Important**

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

14. Optional: Configure any of the following advanced settings.

| Setting | Description | User Actions |
|-----------------|--|------------------|
| Alert threshold | QTS issues a warning notification when the percentage of used volume space is equal to or above the specified threshold. | Specify a value. |

| Setting | Description | User Actions |
|--------------------------------------|---|--|
| Encryption | QTS 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 QTS to automatically unlock and mount the encrypted volume when the NAS starts up. If the encryption key is not saved, you must specify the encryption password each time the NAS restarts. <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> |
| Create a shared folder on the volume | QTS automatically creates the shared folder when the volume is ready. Only the NAS admin account can access the new folder. | Specify a folder name. |

15. Optional: Specify the number of bytes per inode.
The number of bytes per inode determines the maximum volume size and the number of files and folders that the volume can store. Increasing the number of bytes per inode results in a larger maximum volume size, but a lower maximum number of files and folders.
16. Allocate stored space.
Stored space is space used to store a copy of the volume's data locally on the NAS.
 - a. Select a storage pool.
 - b. Specify the capacity of the stored space.

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

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

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

Creating a VJBOD Cloud LUN

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



Note

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

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



Important

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

14. Optional: Configure the sector size.

Changing the sector size to 4 KB increases LUN performance for specific applications and disk types.



Important

VMware does not currently support a 4 KB sector size.

15. Allocate stored space.
Stored space is space used to store a copy of the LUN's data locally on the NAS.
 - a. Select a storage pool.
 - b. Specify the capacity of the stored space.

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

16. Click **Next**.
17. Optional: Deselect **Do not map it to a target for now**.
If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.
18. Review the summary information, and then click **Finish**.

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

Reattaching an Existing VJBOD Cloud Volume



Note

- QTS uses shared folders instead of volumes. For this reason, after creating a VJBOD Cloud volume QTS automatically creates a shared folder with the same name which is stored on the volume. You can then write data to the shared folder.
- When transferring a VJBOD Cloud volume from QuTS hero to QTS, ensure that all files are in subfolders. Files in the shared folder that are not in a subfolder will not be visible in QTS.

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

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

**Note**

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

9. Optional: Click **Performance test**.
QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Attach an existing cloud volume**.
12. Select an existing volume.
13. Allocate stored space.
Stored space is space used to store a copy of the volume's data locally on the NAS.
 - a. Select a storage pool.
 - b. Specify the capacity of the stored space.

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

14. Click **Next**.
15. Optional: Forcibly disconnect the volume from its current NAS.
If a volume is connected to another NAS, then the volume's status will be `Occupied` and **Current NAS** will display an IP address other than `localhost`.

**Warning**

Forcibly disconnecting a volume deletes the volume's data from the other NAS, and then recreates the volume locally from its last restore point. Any changes to data made since the last restore point will be lost.

- a. Specify the admin password of the other NAS.
- b. Click **OK**.
16. Review the summary information, and then click **Finish**.

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

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

Reattaching an Existing VJBOD Cloud LUN

1. Open the **VJBOD Cloud** app.
2. Click **Create VJBOD Cloud Volume/LUN**.
The **Create VJBOD Cloud Volume/LUN** window opens.

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

**Note**

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

9. Optional: Click **Performance test**.
QTS tests the read and write speeds of the cloud space, and then displays the results with a warning if speeds are too low.
10. Click **Next**.
11. Select **Attach an existing cloud LUN**.
12. Select an existing LUN.
13. Allocate stored space.
Stored space is space used to store a copy of the LUN's data locally on the NAS.
 - a. Select a storage pool.
 - b. Specify the capacity of the stored space.

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

14. Click **Next**.
15. Optional: Forcibly disconnect the LUN from its current NAS.
If a volume is connected to another NAS, then the LUN's status will be `Occupied` and **Current NAS** will display an IP address other than `localhost`.

**Warning**

Forcibly disconnecting a LUN deletes the LUN's data from the other NAS, and then recreates the LUN locally from its last restore point. Any changes to data made since the last restore point will be lost.

- a. Specify the admin password of the other NAS.

b. Click **OK**.

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


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

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

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

Connecting to a VJBOD Cloud Service

Refer to this table when configuring a cloud service for a VJBOD Cloud volume or LUN.

| Cloud Service | Steps |
|-------------------|--|
| Alibaba Cloud OSS | <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="border-left: 2px solid #0070C0; padding-left: 10px; 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> |
| 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. |

| Cloud Service | Steps |
|-----------------|---|
| 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. |
| 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. |

| Cloud Service | Steps |
|---------------------------------|---|
| 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. |
| 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. |

| Cloud Service | Steps |
|-------------------|---|
| 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. |
| 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. |

| Cloud Service | Steps |
|---------------|---|
| 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. |
| 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. |

| Cloud Service | Steps |
|---------------------|--|
| 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. |
| 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. |

Overview

The **Overview** screen displays the number of used and total licensed connections, transfer resource information, and information on connected VJBOD Cloud volumes and LUNs. On this screen you can manage VJBOD Cloud volumes and LUNs by selecting one and then clicking **Manage**.

Volume Actions

| Action | Description | Steps |
|-------------------|--|--|
| Resize volume | Increase or decrease the size of the volume. | <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 | QTS 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. |

| Action | Description | Steps |
|----------|---|--|
| Recovery | QTS periodically takes snapshots of a VJBOD Cloud volume. You can use these recovery point snapshots to restore the volume to a previous state. | For details, see VJBOD Cloud Volume and LUN Recovery . |

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 | QTS periodically takes snapshots of a VJBOD Cloud LUN. You can use these recovery point snapshots to restore the LUN to a previous state. | For details, see VJBOD Cloud Volume and LUN Recovery . |




Volume/LUN Connection Status

| Status | Description |
|------------------|--|
| Ready | The cloud storage space is working normally. |
| Syncing | A volume or LUN is currently syncing with the cloud space. |
| License Expiring | The VJBOD Cloud license attached to this storage space will expire within one month. You must renew it if you want to continue using volumes and LUNs in this storage space. |
| 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. |

| Action | Description |
|---------------|--|
| Remove | <p>Remove the volume or LUN from the NAS and delete all of its data from the cloud space.</p> <p> Important If QTS is unable to connect to the cloud service provider, then the volume or LUN will be removed from the local NAS but its data might be left in the cloud space.</p> |
| 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"> • QTS moves all non-uploaded data in the write cache to the cloud space before removing the volume or LUN. This process may take a long time to complete. • If it's not possible to connect to the cloud space, the detach operation will fail. <p>Force Detach: QTS removes the volume or LUN from the local NAS and leaves its data in the cloud space. If it's not possible to connect to the cloud space, QTS will still delete the volume or LUN from the local NAS.</p> <p> Warning If Force Detach is selected, non-uploaded data stored in the volume or LUN might be deleted.</p> |

VJBOD Cloud Volume and LUN Recovery

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

Recovering a VJBOD Cloud Volume or LUN

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



Warning

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

6. Click **Recover**.

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

Transfer Resources

The **Transfer Resources** screen displays the total number of transfer resources allocated to VJBOD Cloud, and the number of transfer allocated to each VJBOD Cloud volume and LUN. On this screen you can manage transfer resources allocation.

Transfer Resource Overview

In VJBOD Cloud, transfer resources correspond to data uploads and downloads. If VJBOD Cloud has 100 total transfer resources, that means the application can create 100 threads for uploading data to and downloading data from the cloud. The total transfer resources allocated to VJBOD Cloud is determined by your NAS hardware.

Transfer Resource Allocation

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

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

Transfer Resource Usage Guidelines

| Problem | Solution |
|--|---|
| VJBOD Cloud is taking a long time to sync data to the cloud. | Increase the total number of transfer resources allocated to VJBOD Cloud. |
| VJBOD Cloud is using too much NAS memory, CPU, or network bandwidth. | Decrease the total number of transfer resources allocated to VJBOD Cloud. |

| Problem | Solution |
|--|---|
| <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

- Go to **VJBOD Cloud > Transfer Resources**.
- 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.

- Click **Apply**.

Configuring Transfer Resources for a Volume or LUN

- Go to **VJBOD Cloud > Transfer Resources**.
- Under **Cloud Volume/LUN Resources**, locate a VJBOD Cloud volume or LUN.
- Configure any of the following settings.

| Setting | Description |
|-----------------|---|
| Reserved | The number of transfer resources reserved for this volume or LUN. |
| Limit | The maximum number of transfer resources this volume or LUN can use.  Note To set this value, Limitation Rule must be set to <i>Limit</i> . |
| Limitation Rule | Select one of the following rules: <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. |

- Click **Apply**.

Event Logs

The **Event Logs** screen displays a log of events, error messages, and warnings related to VJBOD Cloud. On this screen you can view logs by severity level, search logs using keywords, and configure notification settings.

Event Logs
View a log of past events, error messages, and warning messages.

Severity level: All severity levels

| Severity ... | Time | Category | Content |
|----------------|---------------------|-------------|---|
| ⓘ | 2019/10/14 15:26:15 | VJBOD Cloud | [Storage & Snapshots] Detached VJBOD Cloud device "TW-..._CloudVol1". |
| ✖ | 2019/10/14 15:09:48 | VJBOD Cloud | [Storage & Snapshots] Failed to remove VJBOD Cloud device "TW-..._CloudVol1". |
| ⓘ | 2019/10/14 15:09:29 | VJBOD Cloud | [Storage & Snapshots] Started removing VJBOD Cloud device "TW-..._CloudVol1". |
| ✖ | 2019/10/14 15:09:05 | VJBOD Cloud | [Storage & Snapshots] Failed to remove VJBOD Cloud device "TW-..._CloudVol1". |
| ⓘ | 2019/10/14 15:08:53 | VJBOD Cloud | [Storage & Snapshots] Started removing VJBOD Cloud device "TW-..._CloudVol1". |
| ✖ | 2019/09/24 10:18:02 | VJBOD Cloud | [Storage & Snapshots] Failed to remove VJBOD Cloud device "TW-..._CloudVol1". |
| ⓘ | 2019/09/24 10:17:59 | VJBOD Cloud | [Storage & Snapshots] Started removing VJBOD Cloud device "TW-..._CloudVol1". |

Page 1 / 1 | Display item: 1-14, Total: 14 | Show 50 Item(s)

Licenses

The **Licenses** screen displays information about VJBOD Cloud licenses on the NAS. On this screen you can view how many licenses are registered to the local NAS, and how many of those licenses are currently being used. You can also purchase additional VJBOD Cloud licenses.

Licenses
View the status of VJBOD Cloud licenses.

Licensed Connections

Used: 1 Total: 1
Valid: 1 Expired: 0

License Overview

| License Name | Status | Apply Date | Valid Until |
|--------------|--------|------------|-------------|
| Free License | Valid | -- | Perpetual |

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.

7. iSCSI & Fibre Channel

iSCSI & Fibre Channel is a QTS utility that enables you to configure iSCSI and Fibre Channel storage settings on your NAS.

Storage Limits

iSCSI Storage Limits


| iSCSI Storage Limit | Maximum |
|--------------------------------|---|
| iSCSI LUNs and targets per NAS | 255 (combined) |
| Connections per iSCSI session | 8 |
| iSCSI sessions per target | The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth. |
| iSCSI sessions per NAS | The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth. |

Fibre Channel Storage Limits

| Fibre Channel Storage Limit | Maximum |
|-------------------------------------|----------------|
| Fibre Channel ports + port groups | 256 (combined) |
| WWPN aliases | 256 |
| LUN masking rules | 256 |
| Port binding rules | 256 |
| LUNs mapped to 1 Fibre Channel port | 256 |

iSCSI & Fibre Channel Global Settings

You can access global settings by clicking  in the **iSCSI & Fibre Channel** window.

| Setting | Description |
|---|---|
| Enable iSCSI and Fibre Channel services | Enable these services to use iSCSI and Fibre Channel on your NAS. |
| iSCSI service port | View and modify the port that iSCSI initiators connect to.  Tip The default port is 3260. |
| Enable iSNS | SNS enables the automatic discovery and management of iSCSI initiators and targets within a TCP/IP network. iSNS server IP: Specify the IP address of the iSNS server. |

LUNs

QTS LUN Types

QTS supports the following types of LUN.

**Tip**

Block-based LUNs support more features and have faster read/write speeds. QNAP recommends using block-based LUNs over file-based LUNs if possible.

| Feature | Block-based LUN | File-based LUN | VJBOD Cloud LUN |
|--|--|---|--|
| Parent storage space | Storage pool | Thick volume | Cloud space |
| VAAI Full Copy | Supported | Supported | Supported |
| VAAI Block Zeroing | Supported | Supported | Supported |
| VAAI Hardware-Assisted Locking | Supported | Supported | Supported |
| VAAI Thin Provisioning and Space Reclaim | Supported | Not supported | Supported |
| Thin provisioning | Supported | Supported | Not supported |
| QTS space reclamation | Supported (when using VAAI or the host is Windows Server 2012, Windows 8 or later) | Not supported | Supported (when using VAAI or the host is Windows Server 2012, Windows 8 or later) |
| Microsoft ODX | Supported | Not supported | Supported |
| LUN export | Supported | Supported | Supported |
| LUN snapshots | Supported | Partially supported (You can take a snapshot of the LUN's parent volume.) | Supported |
| Read/write speeds | High | Medium to low | High when using caching (stored space) Low when not using caching |


Creating a Block-Based LUN

- Go to one of the following screens.
 - iSCSI & Fibre Channel > iSCSI Storage
 - iSCSI & Fibre Channel > Fibre Channel > FC Storage
- Click **Create**, and then select **New Block-Based LUN**. The **Block-Based LUN Creation Wizard** opens.
- Select the storage pool that this LUN will be created in.
- Select a LUN allocation method.




| Allocation | Description |
|--------------------------|---|
| Thick instant allocation | QTS allocates storage pool space when creating the LUN. This space is guaranteed to be available later. |
| Thin provisioning | QTS allocates storage pool space only when needed, such as when data is being written to the LUN. This ensures efficient use of space but there is no guarantee that space will be available. |

- Click **Next**.

6. Configure the following LUN settings.

| Setting | Description |
|--------------|--|
| LUN name | <ul style="list-style-type: none"> Length: 1 to 32 characters Valid characters: 0-9, a-z, A-Z, underscore (_) |
| LUN capacity | <p>Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method:</p> <ul style="list-style-type: none"> Thick provisioning: Equal to the amount of free space in the parent storage pool. Thin provisioning: 250 TB <p> Tip Select Maximum to allocate all remaining free space to the LUN.</p> |

7. Optional: Configure any of the following advanced settings.

| Setting | Description |
|---|---|
| Sector size | <p>Changing the sector size to 4 KB increases LUN performance for specific applications and disk types.</p> <p> Important VMware does not currently support a 4 KB sector size.</p> |
| Alert threshold | <p>QTS issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold.</p> |
| Accelerate performance with SSD cache | <p>The SSD cache will be used to improve LUN access performance.</p> <p> Important This setting is only available when the SSD cache is enabled.</p> |
| Report volatile write cache for data safety | <p>When enabled, QTS informs iSCSI initiators connected to this LUN that volatile write-cache is being used on the NAS. As a result, initiators might frequently tell QTS to flush cached LUN data to disk, which increases data safety but decreases LUN performance.</p> |
| FUA bit support | <p>When enabled, iSCSI initiators are able to tell QTS to flush important cached data to disk, instead of the whole read-write cache.</p> <p> Important Both the iSCSI initiator and the application using the LUN must support this feature.</p> |

8. Click **Next**.

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

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

10. Click **Finish**.

11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.

For details, see the following topics:

- [Mapping a LUN to an iSCSI Target](#)

- [Mapping a LUN to a Fibre Channel Port Group](#)

Creating a File-Based LUN


1. Go to one of the following screens.
 - **iSCSI & Fibre Channel > iSCSI Storage**
 - **iSCSI & Fibre Channel > Fibre Channel > FC Storage**
2. Click **Create**, and then select **New File-Based LUN**.
The **File-Based LUN Creation Wizard** opens.
3. Select the thick volume that this LUN will be created on.
4. Select a LUN allocation method.


| Allocation | Description |
|--------------------------|---|
| Thick instant allocation | QTS allocates storage pool space when creating the LUN. This space is guaranteed to be available later. |
| Thin provisioning | QTS allocates storage pool space only when needed, such as when data is being written to the LUN. This ensures efficient use of space but there is no guarantee that space will be available. |

5. Click **Next**.
6. Configure the following LUN settings.

| Setting | Description |
|--------------|--|
| LUN name | <ul style="list-style-type: none"> • Length: 1 to 32 characters • Valid characters: 0-9, a-z, A-Z, underscore (_) |
| LUN capacity | Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method: <ul style="list-style-type: none"> • Thick provisioning: Equal to the amount of free space in the parent storage pool. • Thin provisioning: 250 TB |

7. Optional: Configure any of the following advanced settings.

| Setting | Description |
|---|---|
| Sector size | Changing the sector size to 4 KB increases LUN performance for specific applications and disk types.  Important VMware does not currently support a 4 KB sector size. |
| Alert threshold | QTS issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold. |
| Report volatile write cache for data safety | When enabled, QTS informs iSCSI initiators connected to this LUN that volatile write-cache is being used on the NAS. As a result, initiators might frequently tell QTS to flush cached LUN data to disk, which increases data safety but decreases LUN performance. |

| Setting | Description |
|-----------------|---|
| FUA bit support | <p>When enabled, iSCSI initiators are able to tell QTS to flush important cached data to disk, instead of the whole read-write cache.</p> <p> Important Both the iSCSI initiator and the application using the LUN must support this feature.</p> |

8. Click **Next**.
9. Optional: Deselect **Do not map it to a target for now**.
If deselected, the **Edit LUN Mapping** wizard appears after QTS has finished creating the LUN.
10. Click **Finish**.
11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.
For details, see the following topics:
 - [Mapping a LUN to an iSCSI Target](#)
 - [Mapping a LUN to a Fibre Channel Port Group](#)

iSCSI

iSCSI enables computers, servers, other NAS devices, and virtual machines to access NAS storage in the form of LUNs over a TCP/IP network. Hosts can partition, format, and use the LUNs as if they were local disks.

Getting Started with iSCSI

1. Create an iSCSI target on the NAS.
For details, see [Creating an iSCSI Target](#).
2. Create a LUN on the NAS.
A LUN is a portion of storage space, similar to a volume. LUNs are created from storage pool space (block-based) or from space in a thick volume (file-based).
For more information, see:
 - [QTS LUN Types](#)
 - [Creating a Block-Based LUN](#)
 - [Creating a File-Based LUN](#)
3. Map the LUN to the iSCSI target.
Multiple LUNs can be mapped to one target.
For details, see [iSCSI LUN Actions](#).
4. Install an iSCSI initiator application or driver on the host.
The host is the service, computer, or NAS device that will access the LUN.
5. Connect the iSCSI initiator to the iSCSI target on the NAS.



Warning

To prevent data corruption, multiple iSCSI initiators should not connect to the same LUN simultaneously.

The LUNs mapped to the iSCSI target appear as disks on the host.

6. In the host OS, format the disks.

iSCSI Performance Optimization

You can optimize the performance of iSCSI by following one or more of these guidelines:

- Use thick provisioning (instant allocation). Thick provisioning gives slightly better read and write performance than thin provisioning.
- Create multiple LUNs, one for each processor thread on the NAS. For example, if the NAS has four processor threads, then you should create four or more LUNs.



Tip

Go to **Control Panel > System > System Status > System Information > CPU** to view the number of processor threads.

- Use separate LUNs for different applications. For example, when creating two virtual machines which intensively read and write data, you should create one LUN for each VM to distribute the load.
- You can use iSER (iSCSI Extensions for RDMA) for faster data transfers between QNAP NAS devices and VMware ESXi servers. Enabling iSER requires a compatible network card and switch. For a list of compatible network devices, see <https://www.qnap.com/solution/iser>.

iSCSI Storage

The **iSCSI Storage** screen allows you to view iSCSI targets. On this screen you can enable, disable, and edit targets, view each target's mapped LUNs, edit LUN mappings, take snapshots of LUNs, and configure the iSCSI access control list (ACL).



Note

The **Allocated** column displays the space consumption of each LUN. Differences in calculation methods may result in different allocated space values on the NAS and the LUN host.

iSCSI LUNs

Mapping a LUN to an iSCSI Target

1. Go to **iSCSI & Fibre Channel > iSCSI Storage**.
2. Select a LUN.



Tip

Double-click an iSCSI target to view all of its mapped LUNs.

3. Optional: If the LUN is already mapped to a target, disable the LUN.
 - a. Click **Action**, and then select **Disable**.
A confirmation message appears.
 - b. Click **OK**.
QTS disables the LUN.
4. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
5. Select **Map to iSCSI target**.

6. Select an iSCSI target.
7. Optional: Select **Enable LUN**.
If selected, QTS will enable the LUN after mapping it to the target.
8. Click **OK**.

Changing the Target of an iSCSI LUN

1. Go to **iSCSI & Fibre Channel > iSCSI Storage**.
2. Select a mapped LUN.




Tip

Double-click an iSCSI target to view all of its mapped LUNs.

3. Click **Action**, and then select **Disable**.
A confirmation message appears.
4. Click **OK**.
QTS disables the LUN.
5. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
6. Select **Map to iSCSI target**.
7. Select an iSCSI target.
8. Optional: Select **Enable LUN**.
If selected, QTS will enable the LUN after mapping it to the target.
9. Click **OK**.

iSCSI LUN Actions

| LUN Action | Description |
|------------|--|
| Disable | Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators. |
| Enable | Enable the LUN if it is currently disabled. |
| Modify | Edit the LUN settings. |
| Delete | <p>Delete the LUN and all data stored on it.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;"> <p> Important</p> <ul style="list-style-type: none"> This action is only available if the LUN is unmapped. To delete a VJBOD Cloud LUN, use the VJBOD Cloud app. </div> |

| LUN Action | Description |
|-----------------------------|---|
| Edit LUN Mapping | Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: <ul style="list-style-type: none"> Mapping a LUN to a Fibre Channel Port Group Mapping a LUN to an iSCSI Target |
| Show in Storage & Snapshots | Manage the LUN at Storage & Snapshots > Storage > Storage/Snapshots |
| LUN Import/Export | Export the LUN to another server, a local NAS folder, or an external storage device. For details, see LUN Import/Export . |

iSCSI LUN Status

| Status | Description |
|----------|--|
| Enabled | The LUN is active and visible to connected initiators. |
| Disabled | The LUN is inactive and invisible to connected initiators. |

iSCSI Targets

Creating an iSCSI Target

- Go to **iSCSI & Fibre Channel > iSCSI Storage**.
- Click **Create**, and then select **New iSCSI Target**.
The **iSCSI Target Creation Wizard** window opens.
- Click **Next**.
- Specify a target name.
QTS appends the specified name to the iSCSI qualified name (IQN). IQNs are unique names used to identify targets and initiators.
 - Valid characters: 0 to 9, a to z, A to Z
 - Length: 1 to 16 characters
- Optional: Specify a target alias.
An alias enables you to identify the target more easily on the initiator.
 - Length: 1 to 32 characters
 - Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ()
- Optional: Select **Allow clustered access to this target**.
When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously.



Warning

To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.

- Optional: Enable CRC checksums.
Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to

verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

| Checksum Type | Description |
|---------------|---|
| Data Digest | The checksum can be used to verify the data portion of the PDU. |
| Header Digest | The checksum can be used to verify the header portion of the PDU. |

8. Click **Next**.

9. Optional: Enable CHAP authentication.

An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.

- Username
 - Length: 1 to 128 characters
 - Valid Characters: 0 to 9, a to z, A to Z
- Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z

10. Optional: Enable mutual CHAP authentication.

Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.

- Username
 - Length: 1 to 128 characters
 - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
- Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z, all special characters

11. Click **Next**.

12. Optional: Select **Create a LUN and map it to this target**.

If selected, QTS opens the **Block-Based LUN Creation Wizard** immediately after finishing this wizard. The new LUN will then be automatically mapped to this target.


13. Click **Apply**.

QTS creates the iSCSI target, and then opens the **Block-Based LUN Creation Wizard** window if **Create an iSCSI LUN and map it to this target** was enabled.

Editing iSCSI Target Settings

1. Go to **iSCSI & Fibre Channel > iSCSI Storage**.
2. Select an iSCSI target.

3. Click **Action**, and then select **Modify**.
The **Modify iSCSI Target** window opens.
4. Modify any of the following settings.

| Setting | Description |
|--|---|
| Target Alias | <p>An alias enables you to identify the target more easily on the initiator.</p> <ul style="list-style-type: none"> • Length: 1 to 32 characters • Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space () |
| Enable clustered access to the iSCSI target from multiple initiators | <p>When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Warning To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.</p> </div> |
| CRC/Checksum | <p>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.</p> <ul style="list-style-type: none"> • Data Digest: The checksum can be used to verify the data portion of the PDU. • Header Digest: The checksum can be used to verify the header portion of the PDU. |
| Use CHAP authentication | <p>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.</p> <ul style="list-style-type: none"> • Username <ul style="list-style-type: none"> • Length: 1 to 128 characters • Valid Characters: 0 to 9, a to z, A to Z • Password <ul style="list-style-type: none"> • Length: 12 to 16 characters • Valid characters: 0 to 9, a to z, A to Z |

| Setting | Description |
|-------------|--|
| Mutual CHAP | <p>Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.</p> <ul style="list-style-type: none"> • Username <ul style="list-style-type: none"> • Length: 1 to 128 characters • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-) • Password <ul style="list-style-type: none"> • Length: 12 to 16 characters • Valid characters: 0 to 9, a to z, A to Z, all special characters |

5. Click **Apply**.

iSCSI Target Actions

| Action | Description |
|------------------|--|
| Deactivate | Disable an active target and disconnect all connected iSCSI initiators. |
| Activate | Enable a deactivated target. |
| Modify | Edit the target's settings. For details, see Editing iSCSI Target Settings . |
| View Connections | View the IP addresses and IQN information of all iSCSI initiators connected to this target. |
| Delete | Disconnect all connected iSCSI initiators and delete the target. Any LUNs mapped to the target will be unmapped and then added to the unmapped LUN list. |

iSCSI Target Status

| Status | Description |
|-----------|--|
| Ready | The target is accepting connections but no initiators are currently connected. |
| Connected | An initiator is connected to the target. |
| Offline | The target is not accepting connections. |

iSCSI ACL

The iSCSI access control list (ACL) allows you to configure a LUN masking policy for each connected iSCSI initiator. A LUN masking policy determines which LUNs the initiator is able to see and access. If no policy is specified for an iSCSI initiator, then QTS applies the default policy to it.



Tip

- The default policy gives all iSCSI initiators full read/write access to all LUNs.

- You can edit the default policy so that all LUNs are either read-only or not visible to all iSCSI initiators, except for initiators with specific permissions from a policy.

Adding an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Click **iSCSI ACL**.
The **iSCSI ACL** window opens.
3. Click **Add a Policy**.
The **Add a Policy** window opens.
4. Specify the policy name.
The name must consist of 1 to 32 characters from any of the following groups:
 - Letters: a-z, A-Z
 - Numbers: 0-9
 - Special characters: Hyphen (-), space (), underscore (_)
5. Specify the initiator IQN.
6. Configure the access permissions for each LUN.

| Permission | Description |
|-------------|---|
| Read Only | The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data. |
| Read/Write | The iSCSI initiator can read, write, modify, and delete data on the LUN. |
| Deny Access | The LUN is invisible to the iSCSI initiator. |



Tip

Click the values in the columns to change the permissions.

7. Click **Apply**.

Editing an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Click **iSCSI ACL**.
The **iSCSI ACL** window opens.
3. Select a policy.
4. Click **Edit**.
The **Modify a Policy** window opens.
5. Optional: Edit the policy name.
The name must consist of 1 to 32 characters from any of the following groups:
 - Letters: a-z, A-Z
 - Numbers: 0-9
 - Special characters: Hyphen (-), space (), underscore (_)

- Optional: Configure the access permissions for each LUN.

| Permission | Description |
|-------------|---|
| Read Only | The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data. |
| Read/Write | The iSCSI initiator can read, write, modify, and delete data on the LUN. |
| Deny Access | The LUN is invisible to the iSCSI initiator. |



Tip

Click the values in the columns to change the permissions.

- Click **Apply**.

Deleting an iSCSI LUN Masking Policy

- Go to **iSCSI & Fibre Channel > iSCSI Storage**.
- Click **iSCSI ACL**.
The **iSCSI ACL** window opens.
- Select a policy.
- Click **Delete**.
A confirmation message appears.
- Click **OK**.

iSCSI Target Authorization

Each iSCSI target can be configured either to allow connections from all iSCSI initiators, or to only allow connections from a list of authorized initiators.



Important

By default, iSCSI target authorization is disabled.

Configuring an iSCSI Target's Authorized Initiators List

- Go to **iSCSI & Fibre Channel > iSCSI Storage**.
- Select an iSCSI target.
- Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
- Click **Initiators**.
- Select **Allow connections from the list only**.
- Optional: Add one or more iSCSI initiators to the authorized iSCSI initiators list.
 - Click **Add**.
 - Specify the initiator IQN.
 - Click **Confirm**.
 - Repeat the previous steps for each additional iSCSI initiator that you want to add.

7. Optional: Delete one or more iSCSI initiators from the authorized iSCSI initiators list.
 - a. Select an initiator IQN.
 - b. Click **Delete**.
 - c. Repeat the previous steps for each additional iSCSI initiator that you want to delete.
8. Click **Apply**.

Enabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow connections from the list only**.
6. Add one or more iSCSI initiators to the authorized iSCSI initiators list.
 - a. Click **Add**.
 - b. Specify the initiator IQN.
 - c. Click **Confirm**.
7. Repeat the previous step for each additional iSCSI initiator that you want to add.
8. Click **Apply**.

Disabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow all connections**.
6. Click **Apply**.

QNAP Snapshot Agent

QNAP Snapshot Agent enables QTS to take application-consistent snapshots of iSCSI LUNs on VMware or Microsoft servers. Application-consistent snapshots record the state of running applications, virtual machines, and data. When QTS takes a LUN snapshot, QNAP Snapshot Agent triggers the following actions:

- Windows: The server flushes data in memory, logs, and pending I/O transactions to the LUN before the snapshot is created.

- VMware: The server takes a virtual machine snapshot.

**Tip**

To download QNAP Snapshot Agent, go to <https://www.qnap.com/utilities>.

Snapshot Agent Server List

To view a list of all iSCSI initiators that are using QNAP Snapshot Agent with this NAS, go to **iSCSI & Fibre Channel > iSCSI Storage** . Click **Snapshot**, and then select **Snapshot Agent**.

**Tip**

To unregister an iSCSI initiator, select it in the list and then click **Remove**.

Snapshot Agent
✕

Registered Snapshot Agent List <https://www.qnap.com/utility>

| Agent IP/FQDN | Agent... | Client OS | NAS LUN info | Status |
|---------------|----------|---------------------------------|--------------|--------|
| 172.17.48.71 | 1.3.052 | Microsoft Windows NT 6.2.9200.0 | LUN_1 (E:\) | Online |

⏪ ⏩ | Page /1 | ⏪ ⏩ | ↻

Display item: 1-1, Total: 1 | Show Item(s)

Fibre Channel

FC Ports

The **Fibre Channel (FC) Ports** screen displays all of the Fibre Channel ports and port groups on the NAS.

Fibre Channel Port Groups

A Fibre Channel port group is a group of one or more Fibre Channel ports. Fibre Channel port groups help you organize and manage LUN mappings more easily. When a LUN is mapped to a Fibre Channel port group, QTS automatically maps the LUN to every Fibre Channel port in the group.

**Important**

- Each Fibre Channel port can be in one or more Fibre Channel port groups.
- Each LUN can only be mapped to one Fibre Channel group.

- There is a default port group that contains all Fibre Channel ports.

Creating a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Ports**.
2. Click **Create Port Group**.
The **Create Port Group** window opens.
3. Specify a group name.
Name requirements:
 - Length: 1–20 characters
 - Valid characters: A–Z, a–z, 0–9
4. Select one or more Fibre Channel ports.
5. Click **Create**.

Mapping a LUN to a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Storage**.
2. Select a LUN.
3. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
4. Select **Map to FC port group**.
5. Select a Fibre Channel port group.



Tip

The default group contains all Fibre Channel ports.

6. Choose whether you want to configure LUN masking.

| Option | Description |
|--|--|
| Enable LUN and do not configure LUN masking | Do not configure LUN masking. Any initiator that is able to connect to a Fibre Channel port in the port group will be able to see the LUN. |
| Keep LUN disabled and configure LUN masking in the next step | Configure LUN masking. You can restrict which initiators can see the LUN. |

7. Click **OK**.
8. Optional: Configure LUN masking.
 - a. Add one or more initiator WWPNs to the LUN's authorized initiators list.

| Method | Steps |
|--------------------|---|
| Add from WWPN list | <ol style="list-style-type: none"> 1. Select one or more initiator WWPNs in the WWPN list. 2. Click Add. |

| Method | Steps |
|-------------------|---|
| Add WWPNs as text | <ol style="list-style-type: none"> Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> XXXXXXXXXXXXXXXXXXXX XX:XX:XX:XX:XX:XX:XX:XX Click Add. |

- Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases**.
- Optional: Select **Enable LUN**.
If selected, QTS will enable the LUN after mapping it to the target.
- Click **OK**.

Fibre Channel Port Actions

| Action | Description |
|-------------------|--|
| Edit Alias | Specify an alias for the Fibre Channel port. The alias must consist of 1 to 20 characters from any of the following groups: <ul style="list-style-type: none"> Letters: A-Z, a-z Numbers: 0-9 Special characters: Hyphen (-), underscore (_) |
| View initiators | View a list of all Fibre Channel initiators currently logged into the port. |
| Edit port binding | Modify the port binding for the port. Port binding allows you to restrict which initiators are allowed to connect to the port. For more information, see Fibre Channel Port Binding . |

Fibre Channel Port Status

| Status | Description |
|--------------|--|
| Connected | The port has an active network connection. |
| Disconnected | The port does not have an active network connection. |

Fibre Channel Port Binding

Port binding is a Fibre Channel security method that enables you to restrict which initiator WWPNs are allowed to connect through a Fibre Channel port. It is similar to iSCSI target authorization.



Tip

By default, port binding is disabled on all Fibre Channel ports.

Configuring Fibre Channel Port Binding

- Go to **iSCSI & Fibre Channel > Fibre Channel > FC Ports**.
- Select a Fibre Channel port.

3. Click **Action**, and then select **Edit Port Binding**.
The **Fibre Channel Port Binding** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

| Method | Steps |
|--------------------|---|
| Add from WWPN list | <ol style="list-style-type: none"> a. Select one or more initiator WWPNs in the WWPN list. b. Click Add. |
| Add WWPNs as text | <ol style="list-style-type: none"> a. Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • xxxxxxxxxxxxxxxxxxxx • xx : xx : xx : xx : xx : xx : xx : xx b. Click Add. |

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases**.
6. Click **OK**.

FC Storage

The **FC Storage** screen displays the LUN and Fibre Channel port group mappings.

Fibre Channel LUN Masking

LUN masking is a security feature that enables you to make a LUN visible to some Fibre Channel initiators and invisible to other initiators.

Configuring Fibre Channel LUN Masking

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Storage**.
2. Select a LUN.



Important

The LUN must be disabled.

3. Click **LUN Masking**.
The **LUN Masking** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

| Method | Steps |
|--------------------|---|
| Add from WWPN list | <ol style="list-style-type: none"> a. Select one or more initiator WWPNs in the WWPN list. b. Click Add. |

| Method | Steps |
|-------------------|---|
| Add WWPNs as text | <p>a. Specify one WWPN per line using any of the following formats:</p> <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX : XX : XX : XX : XX : XX : XX : XX <p>b. Click Add.</p> |

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List.**


When selected, QTS will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .

6. Select **Enable LUN.**

If selected, QTS will enable the LUN after mapping it to the target.

7. Click **OK.**

Fibre Channel LUN Actions

| LUN Action | Description |
|-----------------------------|---|
| Edit LUN Mapping | <p>Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics:</p> <ul style="list-style-type: none"> • Mapping a LUN to a Fibre Channel Port Group • Mapping a LUN to an iSCSI Target |
| Edit LUN Masking | <p>LUN masking is an authorization method that makes a Logical Unit Number (LUN) visible to some initiators and invisible to other initiators. For details, see Configuring Fibre Channel LUN Masking.</p> |
| Show in Storage & Snapshots | <p>Manage the LUN at Storage & Snapshots > Storage > Storage/ Snapshots</p> |
| Modify | <p>Edit the LUN settings.</p> |
| Enable | <p>Enable the LUN if it is currently disabled.</p> |
| Disable | <p>Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.</p> |
| Delete | <p>Delete the LUN and all data stored on it.</p> <p> Important This action is only available if the LUN is unmapped.</p> |
| LUN Import/Export | <p>Export the LUN to another server, a local NAS folder, or an external storage device. For details, see Creating a LUN Export Job.</p> |

Fibre Channel LUN Status

| Status | Description |
|----------|--|
| Enabled | The LUN is active and visible to connected initiators. |
| Disabled | The LUN is inactive and invisible to connected initiators. |

FC WWPN Aliases

On the **FC WWPN Aliases** screen, you can view, edit, and add WWPNs and WWPN aliases. A WWPN (World Wide Port Name) is a unique identifier for Fibre Channel ports. A WWPN alias is a unique human-readable name for a Fibre Channel port that makes it easier to identify it.

Adding WWPNs

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Click **Add**.
The **Add WWPN** window appears.
3. Add one or more WWPNs to the list of known WWPNs using any of the following methods.

| Method | Steps |
|--|---|
| Add WWPNs from logged-in Fibre Channel initiators. | Select Add WWPNs from all logged-in FC initiators . |
| Add WWPNs as text | Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX:XX:XX:XX:XX:XX:XX:XX |

4. Click **Add**.

Configuring a WWPN Alias

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Locate a WWPN.
3. Under **Alias**, specify an alias for the WWPN.
The alias must consist of 1 to 20 characters from any of the following groups:
 - Letters: A-Z, a-z
 - Numbers: 0-9
 - Special Characters: Underscore (_), hyphen (-)
4. Click **Save**.

Removing a WWPN Alias

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Locate a WWPN.
3. Clear the **Alias** field.
4. Click **Save**.

Exporting a List of WWPN Aliases

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .

2. Click **Export**.
The file browser window opens.
3. In the file browser window, navigate to the folder where you want to save the file.
4. Specify a filename.
5. Click **Save**.

The list of WWPN aliases is saved to your local computer as a CSV file, in the format:

- Field 1: WWPN
- Field 2: Alias

```
11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2
```

Example CSV Output

Importing a List of WWPN Aliases

You can import a list of WWPNs and aliases from a CSV file in the following format:

- Field 1: WWPN
- Field 2: Alias

```

11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2

```

Example CSV File



Important

- Identical aliases will be overwritten from the CSV file.
- Lines not formatted correctly will be ignored.

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Click **Import**.
The file browser window opens.
3. Locate and open the CSV file.

LUN Import/Export

With LUN Import/Export, you can back up a LUN as an image file to an SMB or NFS file server, local NAS folder, or external storage device. You can then import the LUN image file and restore the LUN on any QNAP NAS.

Creating a LUN Export Job

1. Go to **iSCSI & Fibre Channel > LUN Import/Export** .
2. Click **Create a Job**.
The **Create LUN Export Job** windows opens.
3. Select **Export a LUN**.
4. Select a LUN.
5. Optional: Specify a job name.
The name must consist of 1 to 55 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9

- Special characters: Underscore (_)

6. Click **Next**.

7. Select the destination folder.

| Option | Description | Required Information |
|--------------------------|--|--|
| Linux Share (NFS) | NFS share on an external server | <ul style="list-style-type: none"> • IP address or host name • NFS folder or path |
| Windows Share (CIFS/SMB) | CIFS/SMB share on an external server | <ul style="list-style-type: none"> • IP address or host name • Username • Password • CIFS/SMB folder or path |
| Local Host | Local NAS shared folder or connected external storage device | <ul style="list-style-type: none"> • NAS shared folder or external device • Sub-folder |

8. Click **Next**.

9. Optional: Specify a LUN image name.

- The name must consist of 1 to 64 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Underscore (_), hyphen (-), space ()
- The name cannot begin or end with a space.

10. Optional: Select **Use Compression** to compress the image file.

When enabled, the image file will be smaller but exporting will take longer and will use more processor resources.

11. Select when the job will run.

| Option | Description |
|--|--|
| Now | Run the job immediately after the job has been created. After this first run, the job will only run when manually started. |
| <ul style="list-style-type: none"> • Hourly • Daily • Weekly • Monthly | Run the job periodically according to the specified schedule. |

12. Click **Next**.

13. Click **Apply**.


QTS creates the job. The job then starts running if **Now** was selected as the scheduling option.

Importing a LUN from an Image File

1. Go to **iSCSI & Fibre Channel > LUN Import/Export**.
2. Click **Create a Job**.
The **Create LUN Export Job** windows opens.
3. Select **Import a LUN**.
4. Optional: Specify a job name.
The name must consist of 1 to 55 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Underscore (_)
5. Click **Next**.
6. Select the source folder.

| Option | Description | Required Information |
|--------------------------|--|--|
| Linux Share (NFS) | NFS share on an external server | <ul style="list-style-type: none"> • IP address or host name • NFS folder or path |
| Windows Share (CIFS/SMB) | CIFS/SMB share on an external server | <ul style="list-style-type: none"> • IP address or host name • Username • Password • CIFS/SMB folder or path |
| Local Host | Local NAS shared folder or connected external storage device | NAS shared folder or external device |

7. Click **Next**.
8. Select the LUN image file.
9. Click **Next**.
10. Specify the import destination.

| Option | Description | Required Information |
|------------------------|---|--|
| Overwrite existing LUN | Import the image file data to an existing LUN.  Warning All existing data on the LUN will be overwritten. | An existing LUN with the same type (block-based or file-based) as the LUN being imported |
| Create a new LUN | Import the image file as a new LUN. | <ul style="list-style-type: none"> • LUN name • LUN location. This will be a storage pool or volume. |

11. Click **Next**.

12. Click **Apply.**

QTS creates the job, and then immediately runs it.

LUN Import/Export Job Actions

| Action | Description |
|-----------|---|
| Edit | Edit the job. |
| Delete | Delete the job. |
| Start | Start the job. |
| Stop | Stop a running job. |
| View Logs | View the job's status, properties, details of its last run, and event logs. |

LUN Import/Export Job Status

| Action | Description |
|--------------|--|
| -- | The job has not run yet. |
| Initializing | The job is preparing to run. |
| Processing | The job is running. The job's progress is displayed a percentage next to the status. |
| Finished | The job has finished running or was canceled by a user. |
| Failed | The job failed. View the job's event log for details. |

8. SSD Profiling Tool

SSD Profiling Tool controls the creation and execution of SSD over-provisioning tests. These tests help determine the optimum amount of SSD over-provisioning to set when creating an SSD RAID group.

SSD Over-Provisioning

When an SSD is full, the disk's firmware frees up space in a process called garbage collection. Garbage collection results in an effect called write amplification, which reduces the lifespan and random write performance of the SSD. Write amplification can be reduced by over-provisioning, which means reserving space on the disk for garbage collection. Most SSDs are manufactured with 7% or more of their capacity reserved for over-provisioning.

SSD Extra Over-Provisioning

SSD Extra Over-Provisioning enables to you reserve additional space for over-provisioning at the RAID level when creating an SSD RAID group in QTS. Reserving extra space can increase the consistent random write performance and lifespan of the SSD group.



Important

- Space reserved for SSD Extra Over-Provisioning cannot be used for data storage. The total storage capacity of the SSD RAID group will be reduced by the specified amount.
- SSD Extra Over-Provisioning can only be enabled during RAID group creation.
- After creating a RAID group with SSD Extra Over-Provisioning enabled, you can disable the feature or decrease the amount of reserved space. It is not possible to increase reserved space.
- Results will vary depending on the SSD model. Enabling SSD Extra Over-Provisioning may have no effect on some SSDs.

SSD Over-Provisioning Tests

During an SSD over-provisioning test, SSD Profiling Tool first fills the SSDs with random data. It then tests the random write performance of the SSDs over several test phases, each using a different amount of over-provisioning. For example, if a test is created with a test range of 0-20% and a test interval of 5%, SSD Profiling Tool will test SSD write performance in 5 phases, with over-provisioning set to 0%, 5%, 10%, 15%, and 20%. If the random write performance of the disk is very low during any phase, SSD Profiling Tool will end the phase early and move to the next one.

Creating an SSD Over-Provisioning Test

1. Go to **SSD Profiling Tool > Review** .
2. Click **+ Create Test**.
The **Create SSD Test** wizard opens.
3. Click **Next**.
4. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important

- You cannot select disks from multiple expansion units.


- Select one or more disks.
Selecting a single SSD determines the optimum amount of over-provisioning for all SSDs of the same model and capacity. Selecting multiple SSDs determines the optimum amount of over-provisioning for that specific combination of disks and RAID type. Testing multiple disks gives more accurate results, but takes significantly longer than testing a single disk.



Warning

All data on the selected disks will be deleted.

- Select a RAID type.
- Click **Next**.
- Optional: Configure the test settings.

| Setting | Description |
|---|---|
| Test data size | SSD Profiling Tool writes the specified amount of test data to the SSD during each test phase. Decreasing the test data size decreases test time but gives less accurate results. |
| Over-provisioning test range | Specific the minimum and maximum amount of over-provisioning to test. |
| Test interval | Specific over-provisioning increments to test. |
| End a test phase early if consistent performance is too low | <p>SSD Profiling Tool will end a test phase after 5 minutes of testing if the random write speeds during the phase are lower than a system-defined threshold.</p> <p> Tip Enabling this avoids wasting time testing disks when the specified amount of over-provisioning is producing no measurable benefits.</p> |

- Review the estimated time required.
For multiple SSDs, the test may take more than 24 hours.



Tip

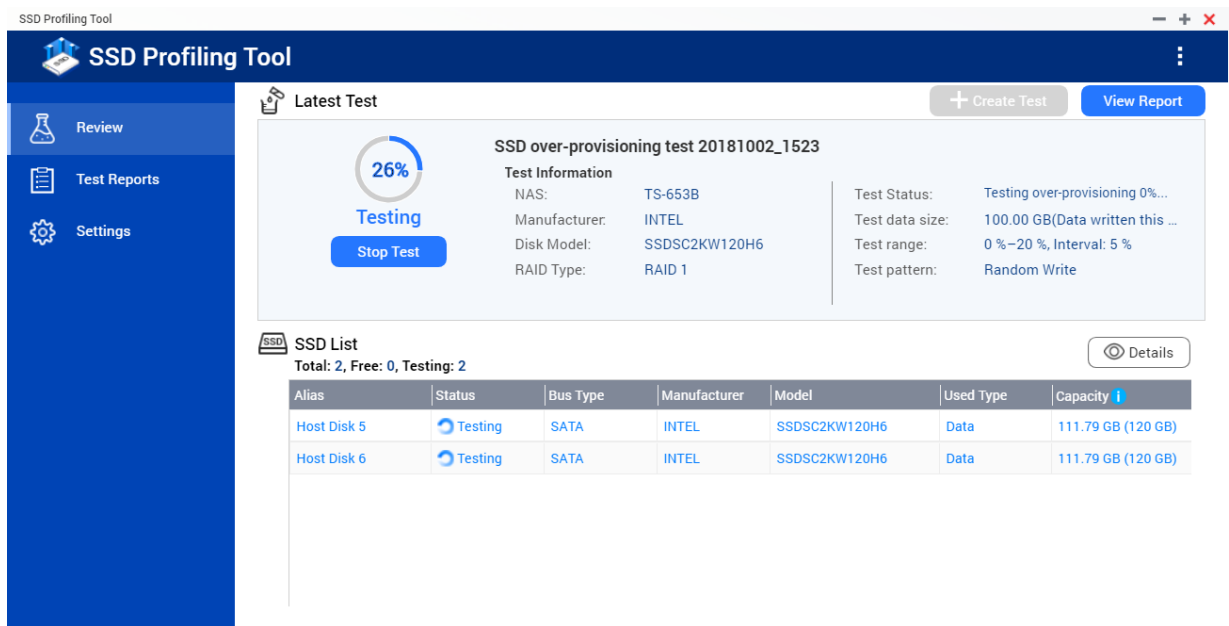
If the estimated test time is too long, reduce the test range, test interval or the test data size.

- Click **Next**.
- Verify the test information.
- Click **Finish**.
A confirmation message appears.
- Click **OK**.

SSD Profiling Tool creates and starts running the test. The test appears as a background task in QTS.

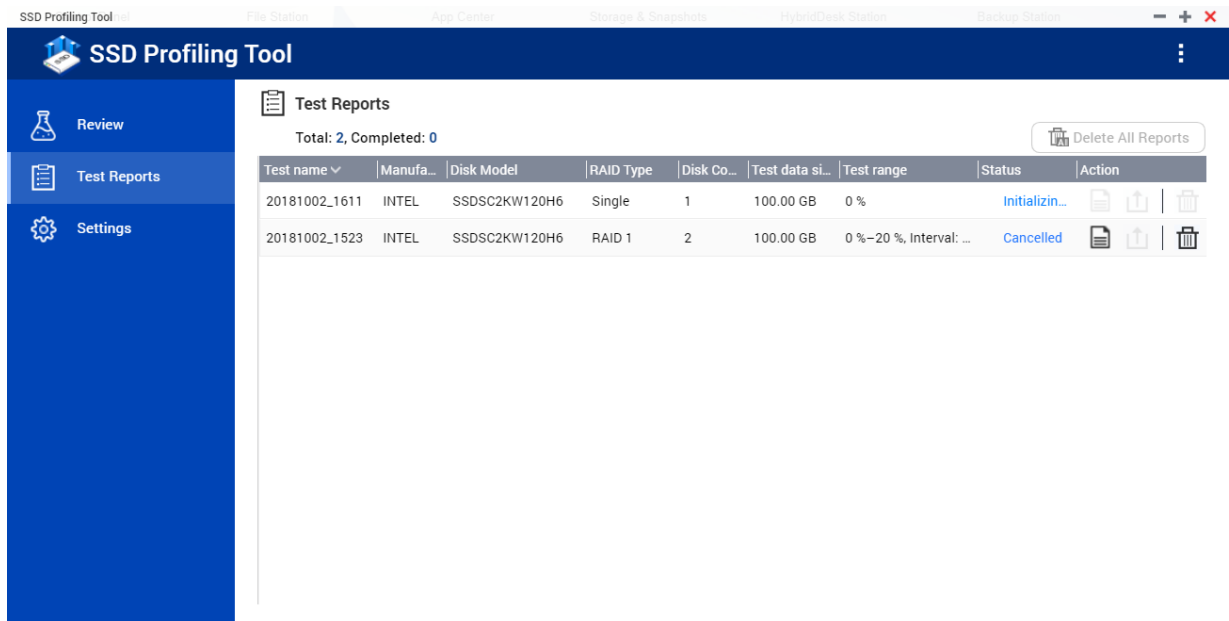
Review

This screen controls the creation and management of SSD tests and displays information about SSDs installed in the NAS.




Test Reports

On this screen you can view, export, and delete test results.




Test Report Actions

| Icon | Description |
|------|---|
| | Open the report in a new window. |
| | Download a copy of the report in XLSX format. |

| Icon | Description |
|---|--------------------|
|  | Delete the report. |

Test Report Information

| Section | Description |
|--------------------------------------|---|
| Test Information | View information about the NAS, the disks being tested, and the settings used in this test. |
| Test Result | View the test results as a graph. Choose from the following views: <ul style="list-style-type: none"> • IOPS / Time • IOPS / Data Written • Data Written / Time <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 10px;"></div> <div> <p>Tip Use these graphs to compare what effect different amounts of over-provisioning had on random write speeds (IOPS).</p> </div> </div> |
| Over-Provisioning Evaluation Results | Enter an IOPS value in Target write performance . SSD Profiling Tool will recommend the amount of over-provisioning needed to consistently achieve the target random write performance. |
| Temperature | View the temperature of the SSDs during each test phase. |
| Test RAID Group | View information about the test SSD RAID group. Details include the RAID type, number of disks, model and capacity of each disk, and disk read/write performance. |

Settings

| Setting | Description |
|---------------------------|--|
| Maximum number of reports | SSD Profiling Tool retains the specified number of reports. Creating additional reports deletes the oldest ones. |


9. Hybrid Backup Sync

About Hybrid Backup Sync

Hybrid Backup Sync (HBS 3) is a comprehensive data backup and disaster recovery solution. Integrating backup, restoration, and synchronization functions, HBS 3 supports a wide range of local, remote server, and cloud storage services.




Configuring HBS 3 Settings





Depending on your data backup needs, HBS 3 can take up a significant amount of storage resources and also generate large amounts of logs. You can set storage limits first before you start to use HBS 3. You can also create notification rules and review the data privacy policy.

1. Open HBS 3.
2. Click , and then click **Settings**.
The **Settings** window opens.
3. Configure application options.

| Setting | Description |
|---|--|
| Storage usage (%) | Specifies a data storage limit. After meeting this limit, HBS 3 sends a notification. |
| Maximum log size | Specifies the maximum size of log files. Larger log files can contain additional information. The log size cannot exceed 1024 MB. |
| Restart after abnormal termination | When HBS 3 starts, any abnormally terminated jobs will automatically restart. |

4. Configure notifications.
 - a. Go to **Notifications**.
 - b. Configure the notification rules.

| Action | Steps |
|---------------------------------|--|
| Create notification rule | <ol style="list-style-type: none"> 1. Click . The Create event notification rule window opens. 2. Create the rule. <p> Tip For details, please see the Notification Center documentation.</p> <p>Notification Center creates the notification.</p> |
| Enable notification rule | <ol style="list-style-type: none"> 1. Identify a notification rule. 2. Click . Notification Center enables the notification. |

| Action | Steps |
|----------------------------------|---|
| Disable notification rule | <ol style="list-style-type: none"> 1. Identify a notification rule. 2. Click . Notification Center disables the notification. |
| Edit notification rule | <ol style="list-style-type: none"> 1. Identify a notification rule. 2. Click . The Edit Rule for Event Notifications window opens. 3. Edit the rule. <p> Tip For details, please see the Notification Center documentation.</p> <ol style="list-style-type: none"> 4. Click Confirm. Notification Center updates the notification. |
| Delete notification rule | <ol style="list-style-type: none"> 1. Identify a notification rule. 2. Click . Notification Center deletes the notification. |
| View notification history | Click View notification history . The Notifications Queue and History window opens. |

5. Configure the data privacy policy.
 - a. Go to **Data Analytics**.
 - b. Select **I have read and agree to the terms of the Privacy Policy**.
6. Click **OK**.

HBS 3 saves the settings.

Jobs

HBS 3 allows users to create and manage backup, restoration, and synchronization jobs, with a wide range of configuration options such as version management, encryption, data deduplication, and data compression. Jobs can be scheduled to run regularly and in succession. Users can also view detailed reports on each job run and manage incoming jobs.

Backup Jobs

Backup jobs simplify the data backup process by saving and reusing common settings. Backup jobs can run according to complex schedules and be configured with advanced policies and rules.

Creating a Backup Job

1. Open HBS 3.
2. Go to **Backup & Restore**.
3. Click **Create**, and then click **New backup job**. The **Create a Backup Job** window opens.

4. Select the source and destination.

- a. Select the source.



Important

Selecting a folder also selects all files and subfolders located inside.

The window displays the number of folders selected and their total size.

- b. Click **Next**.

- c. Select a storage space.

For more information, see [Storage Spaces](#).

- d. Click **Select**.

- e. Select the destination.

- f. Click **OK**.

5. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

6. Click **Next**.

7. Optional: Configure the schedule settings.

| Option | Description |
|----------------------|--|
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <p>a. Click +. The Schedule window opens.</p> <p>b. Configure the schedule.</p> <p>c. Click OK.</p> |
| Run after job | <p>Runs the job after a linked job finishes running.</p> <p> Note A job must be selected from the Select a job menu.</p> |
| No schedule | Runs only when a user starts the job. |
| Backup now | Runs the job immediately after the job is created. |

8. Optional: Configure the version management settings.

- a. Click **Version Management**.

- b. Click **Enable Version Management**.

| Option | Description |
|--------------------------|--|
| Simple Versioning | <p>Retains the specified number of versions.</p> <ul style="list-style-type: none"> • Retained versions: Retains versions until the specified value is reached. Older versions are removed to make space when necessary. The maximum number of versions is 65536. • Retained days: Retains versions created within the specified number of days. Older versions are removed to make space when necessary. The maximum age of retained versions is 3650 days. |
| Smart Versioning | <p>Retains a backup created during a time period for a specified length of time.</p> <ul style="list-style-type: none"> • Retained hours: At the end of every hour, the earliest backup created that hour becomes the hourly backup. The backup is retained for the specified number of hours and then removed. Hourly backups can be retained for up to 87600 hours. • Retained days: At the end of every day, the earliest backup created that day becomes the daily backup. The backup is retained for the specified number of days and then removed. Daily backups can be retained for up to 3650 days. • Retained weeks: At the end of every week, the earliest backup created that week becomes the weekly backup. The backup is retained for the specified number of weeks and then removed. Weekly backups can be retained for up to 520 weeks. • Retained months: At the end of every month, the earliest backup created that month becomes the monthly backup. The backup is retained for the specified number of months and then removed. Monthly backups can be retained for up to 120 months. |

9. Optional: Configure the data integrity check settings.



Note

- Data integrity checks ensure backup files are not corrupted so they can be restored correctly. For details, see [Data Integrity Check](#).
- If version management is enabled, HBS 3 also checks the data integrity of all backup versions where hash values were previously recorded.
- This feature does not currently support Amazon Glacier, Amazon S3 Glacier Deep Archive, or Azure Archive Storage.



- Click **Data Integrity Check**.
- Configure the schedule for quick checks.



Note

Quick checks are not available for NAS-to-NAS backup jobs where the data deduplication feature QuDedup is disabled (see step on configuring job methods).

| Option | Description |
|-----------------------------------|---|
| No schedule (run manually) | Runs only when a user starts the quick check. |
| Run on the following days | Runs the quick check once per week. |

| Option | Description |
|--------------------------------------|--|
| Run on the following schedule | Runs the quick check on a repeating schedule.  Tip <ul style="list-style-type: none"> You can set the frequency between once per year up to once per month. You can select multiple months. |
| One-time | Runs the quick check on the specified date. |
| Start time | Specifies the time of day to run a quick check.  Note This field is not available when No schedule (run manually) is selected. |

c. Optional: Select **Content Check**.



Important

A content check may download all files temporarily for comparison. Some cloud service providers charge additional fees for download traffic.



Note


- Content checks are unavailable for the following:
 - Jobs created in earlier versions of HBS 3 that do not support data integrity checks
 - NAS-to-NAS jobs with QuDedup disabled where HBS 3 on the destination NAS does not support data integrity checks
- After you enable **Content Check** for the first time, HBS 3 will continue to record MD5 hash values even if you disable it later.


d. Optional: Configure the schedule for content checks.



Note

- This option is only available when **Content Check** is selected.
- If a quick check and a content check are both scheduled to run at the same time, only the content check will run.

| Option | Description |
|--------------------------------------|--|
| No schedule (run manually) | Runs only when a user starts the content check. |
| Run on the following days | Runs the content check once per week. |
| Run on the following schedule | Runs the content check on a repeating schedule.  Tip <ul style="list-style-type: none"> You can set the frequency between once per year up to once per month. You can select multiple months. |
| One-time | Runs the content check on the specified date. |

| Option | Description |
|-------------------|--|
| Start time | Specifies the time of day to run a content check.  Note This option is not available when No schedule (run manually) is selected. |



10. Click **Next**.

11. Optional: Configure job methods.



- a. Click **Methods**.
- b. Select **Enable filters**.
- c. Configure basic filters.

| Filter | Description |
|---|---|
| Exclude symbolic links | Excludes symbolic links from the job. |
| Exclude hidden files and folders | Excludes hidden files and folders from the job. |

- d. Click **Advanced Filters**.
The **Specify the filter criteria** window opens.
- e. Configure the filter criteria.

| Method | Description |
|---|---|
| Exclude files by size | Excludes files smaller and/or larger than the specified sizes. |
| Exclude files by modification date | Excludes files modified before and/or after the specified dates. |
| Exclude files modified more than this number of days ago | Excludes files that were modified more than the specified number of days ago. |
| Include the following file types | Includes only files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |
| Exclude the following file types | Excludes all files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |

- f. Click **OK**.
The **Specify the filter criteria** window closes.
- g. Configure the advanced settings.

| Setting | Description |
|-----------------------------|--|
| Use data compression | <p>Compresses data to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <ol style="list-style-type: none"> 1. Click Settings. The Compression Settings window opens. 2. Specify any excluded file types. Separate entries with a comma. 3. Specify a file size limit. Files smaller than the limit are not compressed. 4. Select a compression ratio. <p> Important Data is compressed using bzip. After compression, the data must be decompressed before it can be used.</p> |
| Use QuDedup | <p>Uses a source-side deduplication process to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <p> Note Enabling or disabling this setting alters the available options under Data Integrity Check, Policies, and Options.</p> |


12. Optional: Configure the job policies.






Note

Some policies are only available with certain destination types.

a. Click **Policies**.

| Policy | Description |
|-----------------------------------|---|
| Use client-side encryption | <p>Encrypts data before sending it to the destination. This can reduce the risk of unauthorized data access.</p> <p> Warning Client-side encryption cannot be disabled, and the password cannot be changed after encryption is applied.</p> <ol style="list-style-type: none"> 1. Select Use client-side encryption. 2. Click Settings. The Client-side encryption window opens. 3. Specify an encryption password. 4. Verify the password. 5. Acknowledge the warning. 6. Click OK. The Client-side encryption window closes. |

| Policy | Description |
|--|---|
| Use rate limits | Limits the transmission speed to reduce bandwidth issues. <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify an operating time. 5. Click OK. The Rate Limits window closes. |
| Use TCP BBR congestion control | Optimizes transmission speeds allowing for higher bandwidth and lower latency. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Only back up updated files | Includes only files with a different modification date or file size. |
| Remove deleted data from the destination | Removes data from the destination if it is also deleted or removed from the source. |
| Deleted file retention (days) | Removes deleted files retained in the destination after the specified number of days. |
| Remove additional files in destination folder | Removes destination data that does not exist in the source folder. Changes to files in the source folder will be mirrored in the destination folder. |
| Preserve ACL and extended attributes | Retains information stored in extended attributes. Restore jobs can recover preserved attributes. |
| Detect sparse files | Uploads only non-null data for sparse files. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note This policy does not apply to data stored in encrypted folders. </div> |
| Exclude symbolic links | Excludes symbolic links located in the paired folder. |
| Include hidden files and folders | Includes all hidden files and folders. |
| Compress files during transmission | Compresses files to lower bandwidth requirements. This can speed up data transfer over a slow data connection, but consumes more CPU resources. |
| Exclude system-generated temp files | Excludes temporary files created by the system. |
| Replicate ACL and extended attributes | Replicates information stored in extended attributes. QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority. <div style="border-left: 2px solid #C00000; padding-left: 10px; margin-top: 10px;">  Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server. </div> |

| Policy | Description |
|---|---|
| Delete source files after transmission | Deletes source files after they are successfully transmitted. This option is only available on one-time backup jobs.  Warning If the data is lost or removed from the destination, it cannot be restored. |
| Do not take a snapshot | Reads data directly from the disk instead of using a snapshot as the backup source. |


13. Optional: Configure the job options.



Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|---|--|
| Maximum log size | Specifies the maximum size of log files. The log file size cannot exceed 1024 MB. |
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Notification trigger | Specifies whether notifications should be sent after a job event. For more information, please see the Notification Center documentation. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |
| Concurrent file processing limit | Specifies how many files to transmit at once.  Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure. |
| Job execution timeout (hours) | Specifies how long the job can run before it times out. |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |
| Destination storage usage limit | Specifies a data storage limit. After meeting this limit, HBS 3 sends a notification. |

14. Optional: Configure the network interface assignment.





Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|--|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |

| Option | Description |
|----------------------|---|
| Default Route | <p>HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.</p> <p> Important This option does not automatically optimize traffic for migration.</p> |
| Manual | <p>You can manually select the network interface from a list.</p> <p> Important This option does not automatically optimize traffic for migration.</p> |

15. Click **Next**.

16. Review the job summary.

17. Click **Create**.

HBS 3 creates the backup job.

Relinking a Backup Job

Relinking allows you to reconnect backup data that was moved, or recreate a completed backup job that was deleted.



Important

To relink backup data on the cloud, the original backup job must have enabled deduplication.

1. Open HBS 3.
2. Go to **Backup & Restore**.
3. Click **Create**, and then click **Relink backup job**.
The **Relink Backup Job** window opens.
4. Locate your backup data.
 - a. Select the storage space where your backup data is located.
For more information, see [Storage Spaces](#).
 - b. Click **Select**.
 - c. Locate and select your backup file.
 - d. Click **Next**.
A confirmation window opens.
 - e. Click **Yes**.



Note



HBS automatically pairs your backup file to the original source folder on your NAS.

5. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

6. Click **Next**.

7. Optional: Configure the schedule settings.

| Option | Description |
|----------------------|---|
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <p>a. Click +. The Schedule window opens.</p> <p>b. Configure the schedule.</p> <p>c. Click OK.</p> |
| Run after job | <p>Runs the job after a linked job finishes running.</p> <p> Note A job must be selected from the Select a job menu.</p> |
| No schedule | Runs only when a user starts the job. |
| Backup now | Runs the job immediately after the job is created. |
| Disable job | Disables the job. Disabled jobs cannot run while this option is selected. |

8. Optional: Configure the version management settings.

a. Click **Version Management**.

b. Click **Enable Version Management**.

| Option | Description |
|--------------------------|--|
| Simple Versioning | <p>Retains the specified number of versions.</p> <ul style="list-style-type: none"> • Retained versions: Retains versions until the specified value is reached. Older versions are removed to make space when necessary. The maximum number of versions is 65536. • Retained days: Retains versions created within the specified number of days. Older versions are removed to make space when necessary. The maximum age of retained versions is 3650 days. |

| Option | Description |
|-------------------------|--|
| Smart Versioning | <p>Retains a backup created during a time period for a specified length of time.</p> <ul style="list-style-type: none"> • Retained hours: At the end of every hour, the earliest backup created that hour becomes the hourly backup. The backup is retained for the specified number of hours and then removed. Hourly backups can be retained for up to 87600 hours. • Retained days: At the end of every day, the earliest backup created that day becomes the daily backup. The backup is retained for the specified number of days and then removed. Daily backups can be retained for up to 3650 days. • Retained weeks: At the end of every week, the earliest backup created that week becomes the weekly backup. The backup is retained for the specified number of weeks and then removed. Weekly backups can be retained for up to 520 weeks. • Retained months: At the end of every month, the earliest backup created that month becomes the monthly backup. The backup is retained for the specified number of months and then removed. Monthly backups can be retained for up to 120 months. |

9. Optional: Configure the data integrity check settings.



Note


- Data integrity checks ensure backup files are not corrupted so they can be restored correctly. For details, see [Data Integrity Check](#).
- If version management is enabled, HBS 3 also checks the data integrity of all backup versions where hash values were previously recorded.
- This feature does not currently support Amazon Glacier, Amazon S3 Glacier Deep Archive, or Azure Archive Storage.


- Click **Data Integrity Check**.
- Configure the schedule for quick checks.



Note

Quick checks are not available for NAS-to-NAS backup jobs where the data deduplication feature QuDedup is disabled (see step on configuring job methods).

| Option | Description |
|--------------------------------------|--|
| No schedule (run manually) | Runs only when a user starts the quick check. |
| Run on the following days | Runs the quick check once per week. |
| Run on the following schedule | <p>Runs the quick check on a repeating schedule.</p> <div style="border-left: 2px solid orange; padding-left: 10px; margin-left: 20px;"> <p> Tip</p> <ul style="list-style-type: none"> • You can set the frequency between once per year up to once per month. • You can select multiple months. </div> |
| One-time | Runs the quick check on the specified date. |

| Option | Description |
|-------------------|---|
| Start time | Specifies the time of day to run a quick check.  Note This field is not available when No schedule (run manually) is selected. |

c. Optional: Select **Content Check**.



Important

A content check may download all files temporarily for comparison. Some cloud service providers charge additional fees for download traffic.



Note



- Content checks are unavailable for the following:
 - Jobs created in earlier versions of HBS 3 that do not support data integrity checks
 - NAS-to-NAS jobs with QuDedup disabled where HBS 3 on the destination NAS does not support data integrity checks
- After you enable **Content Check** for the first time, HBS 3 will continue to record MD5 hash values even if you disable it later.

d. Optional: Configure the schedule for content checks.



Note

- This option is only available when **Content Check** is selected.
- If a quick check and a content check are both scheduled to run at the same time, only the content check will run.

| Option | Description |
|--------------------------------------|--|
| No schedule (run manually) | Runs only when a user starts the content check. |
| Run on the following days | Runs the content check once per week. |
| Run on the following schedule | Runs the content check on a repeating schedule.  Tip <ul style="list-style-type: none"> You can set the frequency between once per year up to once per month. You can select multiple months. |
| One-time | Runs the content check on the specified date. |
| Start time | Specifies the time of day to run a content check.  Note This option is not available when No schedule (run manually) is selected. |



10. Click **Next**.

11. Optional: Configure job methods.



- a. Click **Methods**.
- b. Select **Enable filters**.
- c. Configure basic filters.

| Filter | Description |
|---|---|
| Exclude symbolic links | Excludes symbolic links from the job. |
| Exclude hidden files and folders | Excludes hidden files and folders from the job. |

- d. Click **Advanced Filters**.
The **Specify the filter criteria** window opens.
- e. Configure the filter criteria.

| Method | Description |
|---|---|
| Exclude files by size | Excludes files smaller and/or larger than the specified sizes. |
| Exclude files by modification date | Excludes files modified before and/or after the specified dates. |
| Exclude files modified more than this number of days ago | Excludes files that were modified more than the specified number of days ago. |
| Include the following file types | Includes only files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |
| Exclude the following file types | Excludes all files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |

- f. Click **OK**.
The **Specify the filter criteria** window closes.
- g. Configure the advanced settings.

| Setting | Description |
|-----------------------------|--|
| Use data compression | <p>Compresses data to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <ol style="list-style-type: none"> 1. Click Settings. The Compression Settings window opens. 2. Specify any excluded file types. Separate entries with a comma. 3. Specify a file size limit. Files smaller than the limit are not compressed. 4. Select a compression ratio. <p> Important Data is compressed using bzip. After compression, the data must be decompressed before it can be used.</p> |
| Use QuDedup | <p>Uses a source-side deduplication process to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <p> Note Enabling or disabling this setting alters the available options under Data Integrity Check, Policies, and Options.</p> |


12. Optional: Configure the job policies.





Note

Some policies are only available with certain destination types.

a. Click **Policies**.

| Policy | Description |
|-----------------------------------|---|
| Use client-side encryption | <p>Encrypts data before sending it to the destination. This can reduce the risk of unauthorized data access.</p> <p> Warning Client-side encryption cannot be disabled, and the password cannot be changed after encryption is applied.</p> <ol style="list-style-type: none"> 1. Select Use client-side encryption. 2. Click Settings. The Client-side encryption window opens. 3. Specify an encryption password. 4. Verify the password. 5. Acknowledge the warning. 6. Click OK. The Client-side encryption window closes. |

| Policy | Description |
|--|--|
| Use rate limits | Limits the transmission speed to reduce bandwidth issues. <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify an operating time. 5. Click OK. The Rate Limits window closes. |
| Use TCP BBR congestion control | Optimizes transmission speeds allowing for higher bandwidth and lower latency. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Only back up updated files | Includes only files with a different modification date or file size. |
| Remove additional files in destination folder | Removes destination data that does not exist in the source folder. Changes to files in the source folder will be mirrored in the destination folder. |
| Deleted file retention (days) | Removes deleted files retained in the destination after the specified number of days. |
| Preserve ACL and extended attributes | Retains information stored in extended attributes. Restore jobs can recover preserved attributes. |
| Detect sparse files | Uploads only non-null data for sparse files. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;">  Note This policy does not apply to data stored in encrypted folders. </div> |
| Exclude symbolic links | Excludes symbolic links located in the paired folder. |
| Include hidden files and folders | Includes all hidden files and folders. |
| Delete source files after transmission | Deletes source files after they are successfully transmitted. This option is only available on one-time backup jobs. <div style="border-left: 2px solid #C00000; padding-left: 10px; margin-top: 10px;">  Warning If the data is lost or removed from the destination, it cannot be restored. </div> |
| Do not take a snapshot | Reads data directly from the disk instead of using a snapshot as the backup source. |

13. Optional: Configure the job options.




Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|-------------------------|--|
| Maximum log size | Specifies the maximum size of log files. The log file size cannot exceed 1024 MB. |

| Option | Description |
|---|--|
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Notification trigger | Specifies whether notifications should be sent after a job event. For more information, please see the Notification Center documentation. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |
| Concurrent file processing limit | Specifies how many files to transmit at once. <div style="margin-top: 10px;">  Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure. </div> |
| Job execution timeout (hours) | Specifies how long the job can run before it times out. |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |
| Destination storage usage limit | Specifies a data storage limit. After meeting this limit, HBS 3 sends a notification. |



14. Optional: Configure the network interface assignment.



Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route. <div style="margin-top: 10px;">  Important This option does not automatically optimize traffic for migration. </div> |
| Manual | You can manually select the network interface from a list. <div style="margin-top: 10px;">  Important This option does not automatically optimize traffic for migration. </div> |

15. Click **Next**.

16. Review the job summary.

17. Click **Create**.

HBS 3 relinks the backup job.



Data Integrity Check

Data Integrity Check is a feature in HBS 3 that analyzes your backups and attempts to repair any corrupted data. You can run data integrity checks manually, or configure scheduled checks when creating a backup job. HBS 3 offers two types of data integrity checks: quick check and content check.



Tip

Data integrity checks require significant system resources and may take a long time to complete. For the best processing speed, QNAP recommends using an x86-based device with SSDs.

| Feature | | Quick Check | Content Check |
|------------------------------|---------------------------------|---|---|
| Method | | Compares the existence, size, modification time, and/or hash value of each file | <ul style="list-style-type: none"> • NAS-to-NAS backup jobs where HBS 3 on the destination NAS supports data integrity checks: Compares the existence, size, modification time, and hash value of each file • All other jobs: Downloads all files temporarily and calculates hash values for comparison <p> Important Some cloud service providers charge additional fees for download traffic.</p> |
| Supported Jobs | Created in HBS 3 v16 or Later | All backup jobs except NAS-to-NAS jobs with QuDedup disabled | All backup jobs <p> Note For NAS-to-NAS jobs, if the destination NAS runs HBS 3 v15 or earlier, only jobs with QuDedup enabled are supported.</p> |
| | Created in HBS 3 v15 or Earlier | All backup jobs except NAS-to-NAS jobs with QuDedup disabled | None |
| Supported Cloud Destinations | | HBS 3 currently supports all cloud destinations except the following: <ul style="list-style-type: none"> • Amazon Glacier • Amazon S3 Glacier Deep Archive • Azure Archive Storage | |

| Feature | Quick Check | Content Check |
|------------------|---|---|
| Manual checks | <ol style="list-style-type: none"> 1. Open HBS 3. 2. Go to Backup & Restore. 3. Select an existing backup job. 4. Click Check Data Integrity. 5. Click Quick Check. | <ol style="list-style-type: none"> 1. Open HBS 3. 2. Go to Backup & Restore. 3. Select an existing backup job. 4. Click Check Data Integrity. 5. Click Content Check. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p>Note You must enable Content Check in the backup job configuration in order to run a content check. For details, see Creating a Backup Job.</p> </div> |
| Scheduled checks | For details on configuring quick check and content check schedules, see Creating a Backup Job . | |

Restore Jobs

Restore jobs simplify the data recovery process, reducing the effort required to restore data after an incident. You can create a restore job by importing settings from an existing backup job or by specifying the location of your backup data.


Creating a Restore Job from a Backup Job

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing backup job.



Important

The job must have successfully run at least once.

4. Click .
The **Create a Restore Job** window opens.
5. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

6. Optional: Select a backup version.



Note

This option is only available if version management was enabled for the backup job.

- a. Under the backup source, click .

A dialog box opens.

- b. Select a backup version.
- c. Select the source.



Important

Selecting a folder also selects all files and subfolders located inside.

- d. Click **OK**.
The dialog box closes.

7. Select the restoration location.

| Option | Description |
|--------------------------|---|
| Original location | Data is restored to the location it was stored originally. |
| Selected location | Data is restored to a location specified by the user. <ol style="list-style-type: none"> a. Under the destination, click +. A dialog box opens. b. Select the destination. c. Click OK. The dialog box closes. |

8. Optional: Select **Skip deleted data**.



Note

Data marked as deleted will not be restored.

9. Configure the conflict policy.

| Policy | Description |
|----------------------------|--|
| Rename local files | Appends the current date and an iterated number to the end of any duplicate local files. |
| Replace local files | Replaces any duplicate local files with the remote files. |
| Skip files | Skips any duplicate remote files. |

10. Click **Next**.

11. Optional: Configure the schedule settings.

| Option | Description |
|------------------|--|
| Scheduler | Runs the job on a repeating schedule. <div style="margin-top: 10px;"> Important Only 30 schedules can be created per job. </div> <ol style="list-style-type: none"> a. Click +. The Schedule window opens. b. Configure the schedule. c. Click OK. |

| Option | Description |
|----------------------|---|
| Run after job | Runs the job after a linked job finishes running. A job must be selected from the Select a job menu. |
| No schedule | Runs only when a user starts the job. |
| Restore now | Runs the job immediately after the job is created. |

12. Click **Next**.


13. Optional: Configure the job policies.



Note

Some policies are only available with certain destination types.

a. Click **Policies**.

| Policy | Description |
|--|--|
| Use rate limits | Limits the transmission speed to reduce bandwidth issues. <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify an operating time. 5. Click OK. The Rate Limits window closes. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Replicate ACL and extended attributes | QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server.</p> </div> |

14. Optional: Configure the job options.




Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|-------------------------------------|---|
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |

| Option | Description |
|---|--|
| Concurrent file processing limit | Specifies how many files to transmit at once.  Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure. |
| Job execution timeout (hours) | Specifies how long the job can run before it times out. |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |



15. Optional: Configure the network interface assignment.



Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.  Important This option does not automatically optimize traffic for migration. |
| Manual | You can manually select which network interface to use for this job.  Important This option does not automatically optimize traffic for migration. |

16. Click **Next**.

17. Review the job summary.

18. Click **Restore**.


HBS 3 creates the restore job.

Creating a Restore Job from a Destination

If you have run a backup job in HBS 3 before, but the destination of that job—the backup data—is no longer linked to an existing backup job, you can create a restore job by locating the backup data first.

1. Open HBS 3.
2. Go to **Backup & Restore**.
3. Click **Create**, and then click **Restore job**.
The **Create a Restore Job** window opens.
4. Select the storage space where your backup data is located.

13. Optional: Configure the schedule settings.

| Option | Description |
|----------------------|---|
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <ol style="list-style-type: none"> Click +. The Schedule window opens. Configure the schedule. Click OK. |
| Run after job | Runs the job after a linked job finishes running. A job must be selected from the Select a job menu. |
| No schedule | Runs only when a user starts the job. |
| Restore now | Runs the job immediately after the job is created. |


14. Click **Next**.

15. Optional: Configure the job policies.

**Note**

Some policies are only available with certain destination types.

a. Click **Policies**.

| Policy | Description |
|--|--|
| Specify a client-side encryption password | Specifies the encryption password used to access the data. |
| Use rate limits | <p>Limits the transmission speed to reduce bandwidth issues.</p> <ol style="list-style-type: none"> Select Use rate limits. Click Settings. The Rate limit settings window opens. Specify a maximum upload limit. Specify an operating time. Click OK. The Rate Limits window closes. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Replicate ACL and extended attributes | <p>QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority.</p> <p> Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server.</p> |


16. Optional: Configure the job options.



Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|---|--|
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Retries | Specifies the number of times to retry the connection. |
| Retry intervals | Specifies how long to wait between retrying the connection. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs stop. |
| Concurrent file processing limit | Specifies how many files to transmit at once.  Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure. |
| Job execution timeout (hours) | Specifies how long the job can run before it times out. |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |



17. Optional: Configure the network interface assignment.



Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.  Important This option does not automatically optimize traffic for migration. |
| Manual | You can manually select the network interface from a list.  Important This option does not automatically optimize traffic for migration. |

18. Click **Next**.

19. Review the job summary.

20. Click **Restore**.

HBS 3 creates the restore job.

Sync Jobs

Sync jobs synchronize data between locations. Different job types can meet different user needs.

| Job Type | Description |
|--------------|---|
| One-way sync | Data is copied from the NAS to the destination. |
| Active sync | Data is copied from the destination to the NAS. |
| Two-way sync | Data is mirrored between the NAS and the destination. |

Creating a One-Way Sync Job

1. Open HBS 3.
2. Go to **Sync**.
3. Click **Create**, and then click **One-way Sync Job**.
The **Create a Sync Job** window opens.
4. Select a storage space.
For more information, see [Storage Spaces](#).
5. Click **Select**.
6. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

7. Next to **Action**, select the sync action policy.



Note

This option is only available when using a cloud storage space.



| Policy | Description |
|---------------|--|
| Mirror | Copies data from the source to the destination. The source and the destination are identical after synchronization. Any additional data stored in the destination is deleted. |
| Copy | Copies new and updated data from the source to the destination. Deleting the source files does not remove them from the destination. |
| Move | Moves data from the source to the destination. All the source files are removed after completing the sync. |

8. Select the paired folders.





Important

Selecting a folder also selects all files and subfolders located inside.

- a. Under the source, click .
A dialog box opens.
- b. Select a folder.
- c. Click **OK**.
The dialog box closes.
- d. Under the destination, click .
A dialog box opens.
- e. Select a folder.
- f. Click **OK**.
The dialog box closes.
- g. Optional: Repeat the previous steps to add additional paired folders.

**Tip**

- Click  to edit an existing folder.
- Click  to delete an existing pair.

9. Configure the conflict policy.



**Note**


This option is only available when using a cloud storage space.

| Policy | Description |
|-----------------------------|---|
| Rename remote files | Appends the current date and an iterated number to the end of any duplicate remote files. Local files retain their original names. |
| Replace remote files | Replaces any duplicate remote files with the source files. |
| Skip files | Skips any duplicate remote files. |

10. Click **Next**.

11. Optional: Configure the schedule settings.

| Option | Description |
|----------------------------------|--|
| Real-time synchronization | Copies new, modified, or renamed data immediately after changes are made. |
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <ol style="list-style-type: none"> a. Click . The Schedule window opens. b. Configure the schedule. c. Click OK. |

| Option | Description |
|----------------------|---|
| Run after job | Runs the job after a linked job finishes running.  Note A job must be selected from the Select a job menu. |
| No schedule | Runs only when a user starts the job. |
| Sync now | Runs the job immediately after the job is created. |



12. Click **Next**.

13. Optional: Configure job methods.


- a. Click **Methods**.
- b. Select **Enable filters**.
- c. Configure basic filters.

| Filter | Description |
|---|---|
| Exclude symbolic links | Excludes symbolic links from the job. |
| Exclude hidden files and folders | Excludes hidden files and folders from the job. |

- d. Click **Advanced Filters**.
The **Specify the filter criteria** window opens.
- e. Configure the filter criteria.

| Method | Description |
|---|---|
| Exclude files by size | Excludes files smaller and/or larger than the specified sizes. |
| Exclude files by modification date | Excludes files modified before and/or after the specified dates. |
| Exclude files modified more than this number of days ago | Excludes files that were modified more than the specified number of days ago. |
| Include the following file types | Includes only files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |
| Exclude the following file types | Excludes all files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |

- f. Click **OK**.
- g. Configure the advanced settings.

| Setting | Description |
|-----------------------------|--|
| Use data compression | <p>Compresses data to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <ol style="list-style-type: none"> 1. Click Settings. The Compression Settings window opens. 2. Specify any excluded file types. Separate entries with a comma. 3. Specify a file size limit. Files smaller than the limit are not compressed. 4. Select a compression ratio. <p> Important Data is compressed using bzip. After compression, the data must be decompressed before it can be used.</p> |

14. Optional: Configure the job policies.







Note

Some policies are only available with certain destination types.

a. Click **Policies**.

| Policy | Description |
|------------------------|--|
| Use rate limits | <p>Limits the transmission speed to reduce bandwidth issues.</p> <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify a maximum download limit. 5. Specify an operating time. 6. Click OK. The Rate Limits window closes. |

| Policy | Description |
|--|---|
| Use client-side encryption | <p>Encrypts data before sending it to the destination. This can reduce the risk of unauthorized data access.</p> <p> Warning Client-side encryption cannot be disabled, and the password cannot be changed after encryption is applied.</p> <ol style="list-style-type: none"> 1. Select Use client-side encryption. 2. Click Settings. The Client-side encryption window opens. 3. Specify an encryption password. 4. Verify the password. 5. Acknowledge the warning. 6. Click OK. The Client-side encryption window closes. |
| Use TCP BBR congestion control | Optimizes transmission speeds allowing for higher bandwidth and lower latency. |
| Remove additional files in destination folder | Removes destination data that does not exist in the source folder. Changes to files in the source folder will be mirrored in the destination folder. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Detect sparse files | Uploads only non-null data for sparse files. |
| Check file contents | <p>Examines file contents, data, size, and name to determine if two files are identical.</p> <p> Important Selecting this option may increase the time and bandwidth used when syncing data.</p> |
| Exclude duplicate files | <p>Examines file contents, data, size, and name to determine if files are duplicates.</p> <p>Duplicate files are excluded from the job.</p> |
| Exclude symbolic links | Excludes symbolic links located in the paired folder. |
| Include hidden files and folders | Includes all hidden files and folders. |
| Compress files during transmission | <p>Compresses files to lower bandwidth requirements.</p> <p>This can speed up data transfer over a slow data connection, but consumes more CPU resources.</p> |
| Exclude system-generated temp files | Excludes temporary files created by the system. |
| Do not take a snapshot | Reads data directly from the disk instead of using a snapshot as the backup source. |

| Policy | Description |
|--|--|
| Replicate ACL and extended attributes | <p>QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority.</p> <p> Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server.</p> |
| Compare file size and modification date during initial sync | <p>Compares the file size and modification date if the cloud server did not provide a checksum for the destination file. Source files with a different file size or more recent modification date are sent to the destination.</p> |
| Sync Qsync folders only | <p>Only Qsync folders are synced.</p> <p> Note</p> <ul style="list-style-type: none"> This option is only available if the HBS 3 versions on both the source and destination NAS devices support Qsync. This option allows you to back up Qsync folders to a NAS device or restore Qsync folders backed up on the same NAS device. |

15. Optional: Configure the job options.




Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|-------------------------------------|---|
| Maximum log size | Specifies the maximum size of log files. The log file size cannot exceed 1024 MB. |
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Notification trigger | Specifies whether notifications should be sent after a job event. For more information, please see the Notification Center documentation. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Retries | Specifies the number of times to retry the connection. |
| Retry intervals | Specifies how long to wait between retrying the connection. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |

| Option | Description |
|---|--|
| Concurrent file processing limit | Specifies how many files to transmit at once.  Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure. |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |



16. Optional: Configure the network interface assignment.



Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.  Important This option does not automatically optimize traffic for migration. |
| Manual | You can manually select which network interface to use for this job.  Important This option does not automatically optimize traffic for migration. |

17. Click **Next**.

18. Review the job summary.

19. Click **Create**.

HBS 3 creates the sync job.

Creating an Active Sync Job

1. Open HBS 3.
2. Go to **Sync**.
3. Click **Create**, and then click **Active Sync Job**.
The **Create a Sync Job** window opens.
4. Select a storage space.
For more information, see [Storage Spaces](#).
5. Click **Select**.

6. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

7. Next to **Action**, select the sync action policy.



Note

This option is only available when using a cloud storage space.



| Policy | Description |
|---------------|--|
| Mirror | Copies data from the source to the destination. The source and the destination are identical after synchronization. Any additional data stored in the destination is deleted. |
| Copy | Copies new and updated data from the source to the destination. Deleting the source files does not remove them from the destination. |
| Move | Moves data from the source to the destination. All the source files are removed after completing the sync. |

8. Select the paired folders.





Important

Selecting a folder also selects all files and subfolders located inside.

- a. Under the source, click .
A dialog box opens.
- b. Select a folder.
- c. Click **OK**.
The dialog box closes.
- d. Under the destination, click .
A dialog box opens.
- e. Select a folder.
- f. Click **OK**.
The dialog box closes.
- g. Optional: Repeat the previous steps to add additional paired folders.



Tip

- Click  to edit an existing folder.
- Click  to delete an existing pair.

9. Configure the conflict policy.





Note

This option is only available when using a cloud storage space.

| Policy | Description |
|----------------------------|---|
| Rename local files | Appends the current date and an iterated number to the end of any duplicate local files. Remote files retain their original names. |
| Replace local files | Replaces any duplicate local files with the remote files. |
| Skip files | Skips any duplicate remote files. |

10. Click **Next**.

11. Optional: Configure the schedule settings.

| Option | Description |
|----------------------------------|---|
| Real-time synchronization | Copies new, modified, or renamed data immediately after changes are made. |
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <p>a. Click +. The Schedule window opens.</p> <p>b. Configure the schedule.</p> <p>c. Click OK.</p> |
| Run after job | <p>Runs the job after a linked job finishes running.</p> <p> Note A job must be selected from the Select a job menu.</p> |
| No schedule | Runs only when a user starts the job. |
| Sync now | Runs the job immediately after the job is created. |

12. Click **Next**.



13. Optional: Configure job methods.

- a. Click **Methods**.
- b. Select **Enable filters**.
- c. Configure basic filters.

| Filter | Description |
|---|---|
| Exclude symbolic links | Excludes symbolic links from the job. |
| Exclude hidden files and folders | Excludes hidden files and folders from the job. |


- d. Click **Advanced Filters**.
The **Specify the filter criteria** window opens.
- e. Configure the filter criteria.

| Method | Description |
|------------------------------|--|
| Exclude files by size | Excludes files smaller and/or larger than the specified sizes. |

| Method | Description |
|---|---|
| Exclude files by modification date | Excludes files modified before and/or after the specified dates. |
| Exclude files modified more than this number of days ago | Excludes files that were modified more than the specified number of days ago. |
| Include the following file types | Includes only files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |
| Exclude the following file types | Excludes all files of the selected types.  Note When selecting Other , specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*) |



- f. Click **OK**.
The **Specify the filter criteria** window closes.



14. Optional: Configure the job policies.

 **Note**
Some policies are only available with certain destination types.

- a. Click **Policies**.

| Policy | Description |
|------------------------|--|
| Use rate limits | Limits the transmission speed to reduce bandwidth issues. <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify a maximum download limit. 5. Specify an operating time. 6. Click OK. The Rate Limits window closes. |

| Policy | Description |
|--|--|
| Specify a client-side encryption password | <p>Encrypts data before sending it to the destination. This can reduce the risk of unauthorized data access.</p> <p> Warning Client-side encryption cannot be disabled, and the password cannot be changed after encryption is applied.</p> <ol style="list-style-type: none"> 1. Click Settings. The Client-side encryption window opens. 2. Specify an encryption password. 3. Acknowledge the warning. 4. Click OK. The Client-side encryption window closes. |
| Use TCP BBR congestion control | Optimizes transmission speeds allowing for higher bandwidth and lower latency. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize this job's network traffic. |
| Remove additional files in destination folder | Removes destination data that does not exist in the source folder. Changes to files in the source folder will be mirrored in the destination folder. |
| Detect sparse files | Uploads only non-null data for sparse files. |
| Check file contents | <p>Examines file contents, data, size, and name to determine if two files are identical.</p> <p> Important Selecting this option may increase the time and bandwidth used when syncing data.</p> |
| Exclude duplicate files | Examines file contents, data, size, and name to determine if files are duplicates. Duplicate files are excluded from the job. |
| Exclude symbolic links | Excludes symbolic links located in the paired folder. |
| Include hidden files and folders | Includes all hidden files and folders. |
| Compress files during transmission | Compresses files to lower bandwidth requirements. This can speed up data transfer over a slow data connection, but consumes more CPU resources. |
| Exclude system-generated temp files | Excludes temporary files created by the system. |
| Replicate ACL and extended attributes | Replicates information stored in extended attributes. The destination host must enable the same ACL functions and be joined to the same domain. |
| Do not take a snapshot | Reads data directly from the disk instead of using a snapshot as the backup source. |

| Policy | Description |
|--|--|
| Replicate ACL and extended attributes | <p>Replicates information stored in extended attributes. The destination host must enable the same ACL functions and be joined to the same domain. QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority.</p> <p> Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server.</p> |
| Sync Qsync folders only | <p>Only Qsync folders are synced.</p> <p> Note</p> <ul style="list-style-type: none"> • This option is only available if the HBS 3 versions on both the source and destination NAS devices support Qsync. • This option allows you to restore Qsync folders backed up on a different NAS device. |


15. Optional: Configure the job options.



Note

Some options are only available with certain destination types.

a. Click **Options**.

| Option | Description |
|---|--|
| Maximum log size | Specifies the maximum size of log files. The log file size cannot exceed 1024 MB. |
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Notification trigger | Specifies whether notifications should be sent after a job event. For more information, please see the Notification Center documentation. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Retries | Specifies the number of times to retry the connection. |
| Retry intervals | Specifies how long to wait between retrying the connection. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |
| Concurrent file processing limit | <p>Specifies how many files to transmit at once.</p> <p> Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure.</p> |

| Option | Description |
|---|---|
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |



16. Optional: Configure the network interface assignment.



Note

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.  Important This option does not automatically optimize traffic for migration. |
| Manual | You can manually select which network interface to use for this job.  Important This option does not automatically optimize traffic for migration. |

17. Click **Next**.

18. Review the job summary.

19. Click **Create**.

HBS 3 creates the sync job.

Creating a Two-Way Sync Job

1. Open HBS 3.
2. Go to **Sync**.
3. Click **Create**, and then click **Two-way Sync Job**.
The **Create a Sync Job** window opens.
4. Select a storage space.
For more information, see [Storage Spaces](#).
5. Click **Select**.
6. Optional: Specify the job identification information.

| Field | User Action |
|-------------|---|
| Job Name | Specify a job name that does not contain the following characters: / \ : ? < > * " |
| Description | Specify a job description. |

7. Select the paired folders.



Important

Selecting a folder also selects all files and subfolders located inside.

- a. Under the source, click . A dialog box opens.
- b. Select a folder.
- c. Click **OK**. The dialog box closes.
- d. Under the destination, click . A dialog box opens.
- e. Select a folder.
- f. Click **OK**. The dialog box closes.
- g. Optional: Repeat the previous steps to add additional paired folders.



Tip

- Click to edit an existing folder.
- Click to delete an existing pair.



8. Configure the conflict policy.

| Policy | Description |
|------------------------------|---|
| Rename local files | Appends the current date and an iterated number to the end of any duplicate local files. Remote files retain their original names. |
| Replace local files | Replaces any duplicate local files with the remote files. |
| Rename remote files | Appends the current date and an iterated number to the end of any duplicate remote files. Local files retain their original names. |
| Replace remote files | Replaces any duplicate remote files with the source files. |
| Overwrite older files | Replaces any older versions of files. |

9. Click **Next**.

10. Optional: Configure the schedule settings.

| Option | Description |
|----------------------------------|---|
| Real-time synchronization | Copies new, modified, or renamed data immediately after changes are made. |

| Option | Description |
|----------------------|---|
| Scheduler | <p>Runs the job on a repeating schedule.</p> <p> Important Only 30 schedules can be created per job.</p> <p>a. Click +. The Schedule window opens.</p> <p>b. Configure the schedule.</p> <p>c. Click OK.</p> |
| Run after job | <p>Runs the job after a linked job finishes running.</p> <p> Note A job must be selected from the Select a job menu.</p> |
| No schedule | Runs only when a user starts the job. |
| Sync now | Runs the job immediately after the job is created. |


11. Click **Next**.


12. Optional: Configure job methods.

- a. Click **Methods**.
- b. Select **Enable filters**.
- c. Configure basic filters.


| Filter | Description |
|---|---|
| Exclude symbolic links | Excludes symbolic links from the job. |
| Exclude hidden files and folders | Excludes hidden files and folders from the job. |

- d. Click **Advanced Filters**.
The **Specify the filter criteria** window opens.
- e. Configure the filter criteria.

| Method | Description |
|---|--|
| Exclude files by size | Excludes files smaller and/or larger than the specified sizes. |
| Exclude files by modification date | Excludes files modified before and/or after the specified dates. |
| Exclude files modified more than this number of days ago | Excludes files that were modified more than the specified number of days ago. |
| Include the following file types | <p>Includes only files of the selected types.</p> <p> Note When selecting Other, specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*)</p> |

| Method | Description |
|---|---|
| Exclude the following file types | <p>Excludes all files of the selected types.</p> <p> Note When selecting Other, specify the file names or file types. Separate entries with a comma. Use * for wildcard entries. (For example: abc.doc, *.html, test*.*)</p> |

- f. Click **OK**.
The **Specify the filter criteria** window closes.
- g. Configure the advanced settings.




| Setting | Description |
|-----------------------------|--|
| Use data compression | <p>Compresses data to reduce backup sizes and improve transfer speeds and storage efficiency.</p> <ol style="list-style-type: none"> 1. Click Settings. The Compression Settings window opens. 2. Specify any excluded file types. Separate entries with a comma. 3. Specify a file size limit. Files smaller than the limit are not compressed. 4. Select a compression ratio. <p> Important Data is compressed using bzip. After compression, the data must be decompressed before it can be used.</p> |


13. Optional: Configure the job policies.



Note
Some policies are only available with certain destination types.

- a. Click **Policies**.

| Policy | Description |
|--|---|
| Use client-side encryption | <p>Encrypts data before sending it to the destination. This can reduce the risk of unauthorized data access.</p> <p> Warning Client-side encryption cannot be disabled, and the password cannot be changed after encryption is applied.</p> <ol style="list-style-type: none"> 1. Select Use client-side encryption. 2. Click Settings. The Client-side encryption window opens. 3. Specify an encryption password. 4. Verify the password. 5. Acknowledge the warning. 6. Click OK. The Client-side encryption window closes. |
| Use rate limits | <p>Limits the transmission speed to reduce bandwidth issues.</p> <ol style="list-style-type: none"> 1. Select Use rate limits. 2. Click Settings. The Rate limit settings window opens. 3. Specify a maximum upload limit. 4. Specify a maximum download limit. 5. Specify an operating time. 6. Click OK. The Rate Limits window closes. |
| Use TCP BBR congestion control | <p>Optimizes transmission speeds allowing for higher bandwidth and lower latency.</p> |
| Integrate with QuWAN | <p>Allows QuWAN to manage and optimize this job's network traffic.</p> |
| Remove additional files in destination folder | <p>Removes destination data that does not exist in the source folder. Changes to files in the source folder will be mirrored in the destination folder.</p> |
| Detect sparse files | <p>Uploads only non-null data for sparse files.</p> <p> Note This policy does not apply to data stored in encrypted folders.</p> |
| Check file contents | <p>Examines file contents, data, size, and name to determine if two files are identical.</p> <p> Important Selecting this option may increase the time and bandwidth used when syncing data.</p> |
| Exclude symbolic links | <p>Excludes symbolic links located in the paired folder.</p> |

| Policy | Description |
|--|--|
| Include hidden files and folders | Includes all hidden files and folders. |
| Compress files during transmission | Compresses files to lower bandwidth requirements. This can speed up data transfer over a slow data connection, but consumes more CPU resources. |
| Exclude system-generated temp files | Excludes temporary files created by the system. |
| Replicate ACL and extended attributes | <p>QTS and QuTS hero have incompatible ACL settings. If conflicts occur with backup, sync, and restore jobs between QTS and QuTS hero, Windows ACL takes priority.</p> <p> Important To prevent NAS user accounts from having different access permissions, ensure the username and user ID match on both devices, or that both accounts are authenticated from the same AD/LDAP server.</p> |
| Do not take a snapshot | Reads data directly from the disk instead of using a snapshot as the backup source. |


14. Optional: Configure the job options.



Note

Some options are only available with certain destination types.

a. Click **Options**.



| Option | Description |
|---|--|
| Maximum log size | Specifies the maximum size of log files. The log file size cannot exceed 1024 MB. |
| Enable debug logging | Adds the default debug configuration to the log file list when the job is running and generating log files. |
| Notification trigger | Specifies whether notifications should be sent after a job event. For more information, please see the Notification Center documentation. |
| Connection timeout (seconds) | Specifies how long to wait before the connection times out. |
| Retries | Specifies the number of times to retry the connection. |
| Retry intervals | Specifies how long to wait between retrying the connection. |
| Skipped file limit | Specifies a maximum number of files to skip. After exceeding this limit, real-time jobs enter a warning state and scheduled jobs are suspended. |
| Concurrent file processing limit | <p>Specifies how many files to transmit at once.</p> <p> Tip Processing files concurrently can improve the transmission rate, but uses more system resources. Use the default setting if you are unsure.</p> |
| Restart after abnormal termination | Restarts the job if it abnormally terminates while running. |

15. Optional: Configure the network interface assignment.

**Note**

This setting is only available when your NAS has two or more network interface connections. For details, see the Network & Virtual Switch section of the QTS User Guide or the QuTS hero User Guide.

- a. Click **Network**.

| Option | Description |
|------------------------------|---|
| Automatic (Optimized) | HBS 3 selects the least busy and highest-performing network interface. |
| Default Route | <p>HBS 3 selects a network interface based on the packet-forwarding rule for traffic without a specific route.</p> <p> Important This option does not automatically optimize traffic for migration.</p> |
| Manual | <p>You can manually select the network interface from a list.</p> <p> Important This option does not automatically optimize traffic for migration.</p> |

16. Click **Next**.

17. Review the job summary.


18. Click **Create**.

HBS 3 creates the sync job.

Job Management


HBS 3 allows users to perform a wide range of actions on previously created jobs.

Running a Job

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Under **Action**, click .

HBS 3 runs the job.


Stopping a Job

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Under **Action**, click .

HBS 3 stops the job.

Disabling a Job

Disabling prevents a job from being run either manually or automatically.

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Under **Action**, click .
The **Edit a Job** window opens.
5. Go to **Schedule**.
6. Select **Disable job**.




Tip

To reenable the job in the future, deselect this setting.

7. Click **Save**.

HBS 3 disables the job.

Editing a Job

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Under **Action**, click .
The **Edit a Job** window opens.
5. Configure the job settings.



Note

For details, see the related topic:

- [Backup Jobs](#)
- [Restore Jobs](#)
- [Sync Jobs](#)

6. Click **Save**.

HBS 3 edits the job.

Cloning a Job

1. Open HBS 3.
2. Depending on the type of job you want to clone, go to one of the following:
 - **Backup & Restore**

- **Sync**

3. Identify an existing job.
4. Click **Clone Job**.
A job creation window opens.
5. Optional: Configure the job settings.

**Note**

For details, see the related topic:

- [Backup Jobs](#)
- [Restore Jobs](#)
- [Sync Jobs](#)

6. When you reach the **Summary** screen, click **Create**.

HBS 3 clones the job.

Deleting a Job


1. Open HBS 3.
2. Go to **Jobs**.
3. Select an existing job.
4. Click **Delete**.
A confirmation window opens.
5. Click **OK**.





HBS 3 deletes the job.

Job Reports

Job reports provide additional information about job performance. Users can download detailed information about each job run, and also manage certain records for each job.

Viewing Job Reports


1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Click .
The **Report** window opens.
5. Review the job report.

| Tab Name | Description |
|----------|---|
| Results | <p>Lists information about past job runs</p> <p> Tip</p> <ul style="list-style-type: none"> • Under Action, click  to view additional details. • Under Action, click  to download a detailed list of the files impacted by the job run. |
| Logs | <p>Lists information about past job events</p> <p> Tip</p> <p>Click Save to export the full log history.</p> |

Managing Job Report Records

HBS 3 maintains detailed records of the transferred, filtered, and skipped files in every job run. You can configure different rules for each job.

Over time, these records can occupy a significant amount of storage space. Limiting the number of records stored for a job can help you free up storage space.

1. Open HBS 3.
2. Go to **Jobs**.
3. Identify an existing job.
4. Click .
The **Report** window opens.
5. Click **File History Settings**.
The **Settings** window opens.
6. Optional: Configure the rules.

| Rule | Description |
|---|--|
| Delete records older than this number of most recent runs | HBS 3 keeps records for the specified number of job runs. When the number of runs exceeds this value, HBS 3 removes the oldest record. |
| Delete records for runs executed more than this amount of time ago | HBS 3 keeps records for the specified length of time. HBS 3 automatically removes job records older than the specified period. |
| Do not keep records of transferred files | HBS 3 does not keep records of transferred files. |

7. Optional: Delete all file history.



Important






Once all history is deleted, you can no longer export records for previous job runs.

- a. Click **Clear File History**.
A confirmation window opens.
- b. Click **OK**.

HBS 3 deletes all file history.

Incoming Jobs

Incoming jobs are created on a remote NAS and use the local NAS as a source or destination. You can view details and perform various actions on incoming jobs by going to **Jobs > Incoming Jobs** .

| Action | Steps |
|-------------------------|---|
| Filter incoming jobs | <ol style="list-style-type: none"> Next to Filter, click Type / Status. Select a job type or job status to view. <p> Tip To filter by job type and job status simultaneously, select a job type first, then repeat the steps to select a job status.</p> |
| Disable an incoming job | <ol style="list-style-type: none"> Identify an incoming job. Click  . <p> Important This action disables the incoming job on the local device, but not on the remote device. This may result in errors on the remote device.</p> |
| Enable an incoming job | <ol style="list-style-type: none"> Identify an incoming job. Click  . <p>The incoming job can access the local NAS storage.</p> |
| Clear logs | <ol style="list-style-type: none"> Select incoming jobs to remove. Click Clear logs. <p> Note This action only clears the records from the viewing list. The incoming jobs can still access the local NAS.</p> |

Services

HBS 3 provides additional storage services that run on the local NAS. These services include Time Machine backups for Apple devices, rsync and RTRR servers, and configuration of the USB One Touch Copy button for certain QNAP NAS models.

Time Machine

Time Machine is an application built into some Apple devices that can create incremental data backups. The HBS 3 Time Machine service allows an Apple device to store these backups on the NAS.

Configuring Time Machine

- Open HBS 3.
- Go to **Services > Time Machine** .

3. Optional: Select **Shared Time Machine account**.



Note

This option allows the use of a shared account when making Time Machine backups from a Mac to the NAS.

| Setting | Description |
|---------------------|---|
| Display name | The name displayed in the Backups screen. This setting cannot be changed. |
| Username | The shared username used to access the server. This setting cannot be changed. |
| Password | Specifies the password used to access the Time Machine backup data. |
| Volume | Specifies the volume where Time Machine backups are stored. |
| Capacity | Specifies the maximum storage capacity for Time Machine backups. <ul style="list-style-type: none"> • Unlimited: No limit is set. • Maximum: Specifies a maximum limit. |

4. Optional: Select **Local NAS accounts**.



Note

This option allows the use of local NAS accounts when creating Time Machine backups from a Mac to the NAS. For more information, go [here](#).

5. Click **Apply**.

HBS 3 saves the Time Machine configuration.


Time Machine Backups

You can manage Time Machine backups on the NAS by going to **Services > Time Machine > Backups** . You can view backup records by volume and delete selected backups to free up storage space on the NAS.

Rsync Server

The rsync server can transfer and synchronize data across networked computers by comparing the modification times and sizes of files.

Enabling the Rsync Server


1. Open HBS 3.
2. Go to **Services > Rsync Server** .
3. Click  .

HBS 3 enables the rsync server.

Configuring the Rsync Server

1. Open HBS 3.
2. Go to **Services > Rsync Server** .

3. Configure account access settings.

| Option | Description |
|------------------------------------|--|
| Shared rsync server account | <p>This option allows incoming connections to log in with a shared account.</p> <ul style="list-style-type: none"> • Username: Specify a username. • Password: Specify a password. <p> Note The username and password must each contain 1 to 32 characters with the following conditions:</p> <ul style="list-style-type: none"> • Valid characters: A–Z, a–z, 0–9, space () • Valid special characters: . - _ ~ ! @ # \$ % ^ & () { } • Does not start or end with a space () |
| Local NAS accounts | This option allows incoming connections to log in with a local NAS account. |

4. Configure rsync server settings.

| Setting | Description |
|-----------------------------|---|
| Port | Specifies the port number used to access the local NAS. |
| Integrate with QuWAN | <p>Allows QuWAN to manage and optimize network traffic for jobs using this service.</p> <p>This feature is automatically disabled for rsync jobs that have enabled connection encryption (e.g., SSL).</p> |
| Download limit | <p>Sets the download rate limit.</p> <ul style="list-style-type: none"> • Unlimited: No limit is set. • Maximum: Specifies a maximum limit. |


5. Click **Apply**.

HBS 3 saves the rsync server configuration.

RTRR Server

Real-time Remote Replication (RTRR) is a proprietary backup method built into QNAP NAS devices that can create incremental data backups. The HBS 3 RTRR server service allows another QNAP device to store these backups on the local NAS. RTRR improves backup efficiency and reduces backup time.


Enabling the RTRR Server

1. Open HBS 3.
2. Go to **Services > RTRR Server**.
3. Click .

HBS 3 enables the RTRR server.

Configuring the RTRR Server

1. Open HBS 3.
2. Go to **Services > RTRR Server** .
3. Configure account access settings.

| Option | Description |
|-----------------------------------|--|
| Shared RTRR server account | <p>This option allows incoming connections to log in with a shared account.</p> <ul style="list-style-type: none"> • Password: Specify a password. • Verify password: Verify the password. <p> Note The password must contain 1 to 32 characters with the following conditions:</p> <ul style="list-style-type: none"> • Valid characters: A–Z, a–z, 0–9, space () • Valid special characters: . - _ ~ ! @ # \$ % ^ & () { } • Does not start or end with a space () |
| Local NAS accounts | This option allows incoming connections to log in with a local NAS account. |

4. Configure RTRR server settings.

| Setting | Description |
|---------------------------------------|---|
| Port | Specifies the port number used to access the local NAS. |
| Use TCP BBR congestion control | This option optimizes transmissions speeds allowing for higher bandwidth and lower latency. |
| Integrate with QuWAN | Allows QuWAN to manage and optimize network traffic for jobs using this service. |
| Upload limit | <p>Sets the upload rate limit.</p> <ul style="list-style-type: none"> • Unlimited: No limit is set. • Maximum: Specifies a maximum limit. |
| Download limit | <p>Sets the download rate limit.</p> <ul style="list-style-type: none"> • Unlimited: No limit is set. • Maximum: Specifies a maximum limit. |

5. Optional: Configure network access approval.
 - a. Select **Allow approved connections**.



Note

If no IP addresses are added, all connections are allowed.

The **Approved Connections** table appears.

- b. Click **Add**.
The **Add IP Address** window opens.

- c. Select an IP address version.
- d. Specify an IP address, or IP address and subnet mask.
- e. Select an access privilege.
- f. Click **Add**.

6. Click **Apply**.

HBS 3 saves the RTRR server configuration.

Configuring USB One Touch Copy

The USB One Touch Copy button is a physical button with a USB port available on some QNAP NAS models, designed for quick data transfer between the NAS and an external device. HBS 3 allows you to configure the behavior of pressing the button when an external device is connected to the button's USB port.

1. Open HBS 3.
2. Go to **Services > USB One Touch Copy** .
3. Select an operating mode.

| Operating Mode | Description |
|---------------------|---|
| Smart Import | <p>Automatically imports new media from connected devices after pressing the USB One Touch Copy button.</p> <ul style="list-style-type: none"> a. Click Settings. The Smart Import window opens. b. Select a destination. c. Click Apply. |

| Operating Mode | Description |
|-------------------------------|--|
| USB One Touch Copy | <p>Configures advanced actions after pressing the USB One Touch Copy button.</p> <ol style="list-style-type: none"> a. Click Settings. The USB One Touch Copy window opens. b. Select a backup mode. c. Select a backup action. <ul style="list-style-type: none"> • Add directory: Backs up data to a new directory in the destination folder. • Copy: Backs up data to the destination folder. • Synchronize: Copies data from the source to the destination. Any duplicate data in the destination will be overwritten with the source data. Any destination data that does not exist in the source folder will be removed. Select the Efficiently handle sparse files option to skip empty files. d. Select the paired folders. e. Optional: Select Manually unmount USB drive. f. Optional: Select Enable the alarm buzzer. g. Optional: Configure notification rules. <ol style="list-style-type: none"> 1. Click Notifications. 2. Select the job event rules. For more information, please see the Notification Center documentation. h. Click Apply. |
| External Storage Drive | <p>Pressing the USB One Touch Copy button does not copy data to the NAS. Connected devices are still treated as external storage drives.</p> |

4. Click **Apply**.

HBS 3 saves the USB One Touch Copy configuration.

Storage Spaces





Storage spaces store configurations for frequently accessed locations and make them easily available for creating and editing HBS 3 jobs.

Storage Space Creation

HBS 3 allows you to create storage spaces on remote NAS devices, remote servers, and cloud storage services.

Creating a Storage Space on a Remote NAS

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Remote NAS**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|-------------------------------|--|
| Name | The name used to identify the storage space. |
| IP address / Host name | The IP address or hostname used to access the storage space.  Tip Click  to scan for available devices. |
| Port | The port number used to access the storage space. This value must be between 1 to 65535. |
| Account access | The account used to access the storage space. <ul style="list-style-type: none"> • RTRR server account: Uses the shared RTRR server account defined on the remote NAS. • Remote NAS account: Uses a NAS account defined on the remote NAS.  Important Remote access with these account options must first be enabled on the remote NAS or server. |
| Username | The username used to access the storage space.  Note This field is only available if Remote NAS account is selected for account access. |
| Password | The password used to access the storage space. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |

6. Optional: Test the connection.






| Test | Description |
|----------------------|--|
| Detect Server | Tests the accessibility of the selected storage space. |
| Speed Test | Tests the speed of connection to the selected storage space. |

7. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on a Remote Server

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select a remote server.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|------------------------------------|---|
| Name | The name used to identify the storage space. |
| IP address / Host name | The IP address or hostname used to access the storage space.  Tip With CIFS/SMB Servers, click  to scan for available devices. |
| Port | The port number used to access the storage space. This value must be between 1 to 65535. |
| Account access | The account used to access the storage space. <ul style="list-style-type: none"> • Rsync server account: Uses the shared rsync server account defined on the remote NAS. • Remote NAS account: Uses a NAS account defined on the remote NAS.  Important Remote access with these account options must first be enabled on the remote NAS or server. |
| Username | The username used to access the storage space. |
| Password | The password used to access the storage space. |
| Rsync Server Settings | |
| Server Type | The type of server used to access the storage space. |
| Use encryption port | The encryption port used to access the storage space. This value must be between 1 - 65535. |
| FTP Server Settings | |
| FTP with SSL/TLS (Explicit) | Uses an SSL/TLS connection to access the storage space. |
| Enable passive mode | The passive mode used to access the storage space. <ul style="list-style-type: none"> • PASV: Only used with an IPv4 address. • EPSV: Used with any IP address. |
| CIFS/SMB Server Settings | |
| Destination folder | The path to the destination folder.  Note Click  to scan for available folders. |

- Optional: Test the connection.

| Test | Description |
|------------------------|--|
| Test Connection | Tests the accessibility of the selected storage space. |
| Speed Test | Tests the speed of connection to the selected storage space. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Alibaba Cloud

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **Alibaba Cloud**.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Amazon Glacier

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **Amazon Glacier**.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|-------------------------|--|
| Name | The name used to identify the storage space. |
| Service provider | The regional service provider for the cloud service. |

| Setting | Description |
|---------------------------------|--|
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Amazon S3

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Amazon S3 & S3 Compatible**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Service provider | The regional service provider for the cloud service. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use specific bucket | Allows you to control which bucket to use. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Azure Storage

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Azure Storage**.
The **Create a Storage Space** window opens.

5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Storage account | The storage account used to access the cloud service. |
| Access key | The identifier used to sign requests to the cloud service. |
| Region | The region where the cloud service operates. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Backblaze B2

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Backblaze B2**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| keyID | The account used to access the cloud service. |
| Application key | The application key used to access the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Box

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Box**.
A sign-in window opens.

5. Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.
6. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

7. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Catalyst Cloud

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Catalyst Cloud**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Project Name | The name used to identify the storage space. |
| Username | The username used to access the storage space. |
| Password | The password used to access the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Cynny Space

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Cynny Space**.
The **Create a Storage Space** window opens.

5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on DigitalOcean

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **DigitalOcean**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on DreamObjects

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **DreamObjects**.
The **Create a Storage Space** window opens.

- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Dropbox

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **Dropbox**.
A sign-in window opens.
- Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Google Cloud Storage

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **Google Cloud Storage**.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|---|
| Name | The name used to identify the storage space. |
| Project ID | The identifier used to access the project. |
| Authentication | <ul style="list-style-type: none"> • OAuth <ol style="list-style-type: none"> 1. Click Authenticate. A sign-in window opens. 2. Sign in to the cloud service. The sign-in window closes. • P12 Key <ol style="list-style-type: none"> 1. Click Browse. A file browser opens. 2. Locate a key file. 3. Click Open. The file browser closes. 4. Specify the service account email. • JSON Key <ol style="list-style-type: none"> 1. Click Browse. A file browser opens. 2. Locate a key file. 3. Click Open. The file browser closes. 4. Specify the service account email. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Google Drive

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Google Drive**.
A sign-in window opens.
5. Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.

- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on HiCloud

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **HiCloud**.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on HiDrive

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **HiDrive**.
A sign-in window opens.
- Sign in to the cloud service.
A sign-in window opens.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

7. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on HKT Object Storage

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **HKT Object Storage**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Huawei Cloud

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Huawei Cloud**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|-------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |

| Setting | Description |
|---------------------------------|--|
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on HubiC

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **hubiC**.
A sign-in window opens.
5. Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.
6. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

7. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on IBM Cloud

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **IBM Cloud**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|-------------|--|
| Name | The name used to identify the storage space. |

| Setting | Description |
|---------------------------------|--|
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on luckycloud S3

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **luckycloud S3**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on OneDrive & OneDrive for Business

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **OneDrive & OneDrive for Business**.
A sign-in window opens.
5. Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.

6. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

7. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on OpenStack Swift

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **OpenStack Swift**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|------------------------------------|--|
| Name | The name used to identify the storage space. |
| Use Keystone authentication | Allows the configuration of a tenant name or tenant ID. |
| Large object type | The method used to split larger files into smaller pieces. Contact your cloud service provider for more information. |
| User ID | The account used to access the cloud service. |
| API key | The API key used to access the cloud service. |
| Authentication service | The URL used to access the authentication service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Oracle Cloud

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Oracle Cloud**.
The **Create a Storage Space** window opens.

5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Region | The region where the cloud service operates. |
| Namespace | The namespace used to access the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Qcloud IT

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Qcloud IT**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on RackSpace

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **RackSpace**.

The **Create a Storage Space** window opens.

5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| User ID | The account used to access the cloud service. |
| Password | The password used to access the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on SFR Cloud

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **SFR**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on ShareFile

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **ShareFile**.
A sign-in window opens.
5. Sign in to the cloud service.

The sign-in window closes.
The **Create a Storage Space** window opens.

- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on SharePoint

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **SharePoint**.
A sign-in window opens.
- Sign in to the cloud service.
The sign-in window closes.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Wasabi

- Open HBS 3.
- Go to **Storage Spaces**.
- Click **Create**.
A storage space selection window opens.
- Select **Wasabi**.
The **Create a Storage Space** window opens.
- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Access key | The identifier used to sign requests to the cloud service. |
| Secret key | The identifier used to sign requests to the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Use SSL connection | Requires SSL connection when accessing the remote NAS. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on WebDAV

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **WebDAV**.
The **Create a Storage Space** window opens.
5. Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| User ID | The account used to access the cloud service. |
| Password | The password used to access the storage space. |
| Server URL | The URL used to access the cloud service. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

6. Click **Create**.

HBS 3 creates the storage space.

Creating a Storage Space on Yandex Disk

1. Open HBS 3.
2. Go to **Storage Spaces**.
3. Click **Create**.
A storage space selection window opens.
4. Select **Yandex Disk**.
A sign-in window opens.
5. Sign in to the cloud service.
The sign-in window closes.

The **Create a Storage Space** window opens.

- Configure the storage space settings.

| Setting | Description |
|---------------------------------|--|
| Name | The name used to identify the storage space. |
| Use a proxy server | Allows you to use the system proxy server or configure another proxy server. |
| Validate SSL certificate | Verifies the validity of the cloud services SSL certificate. |

- Click **Create**.

HBS 3 creates the storage space.

Editing a Storage Space

- Open HBS 3.
- Go to **Storage Spaces**.
- Select a storage space.

- 

Click  .
The **Edit Storage Space** window opens.

- Configure the storage space settings.
- Click **Save**.

HBS 3 applies the changes.

Deleting a Storage Space

- Open HBS 3.
- Go to **Storage Spaces**.
- Select a storage space.

- 

Click  .
A confirmation message appears.

- Click **OK**.

HBS 3 deletes the storage space.

10. Network & Virtual Switch

About Network & Virtual Switch

Network & Virtual Switch is a QTS utility that centralizes the creation, configuration, and control of network connections. Network & Virtual Switch also manages physical network interfaces, virtual adapters, Wi-Fi, and Thunderbolt connections in addition to controlling DHCP, DDNS, and gateway services.

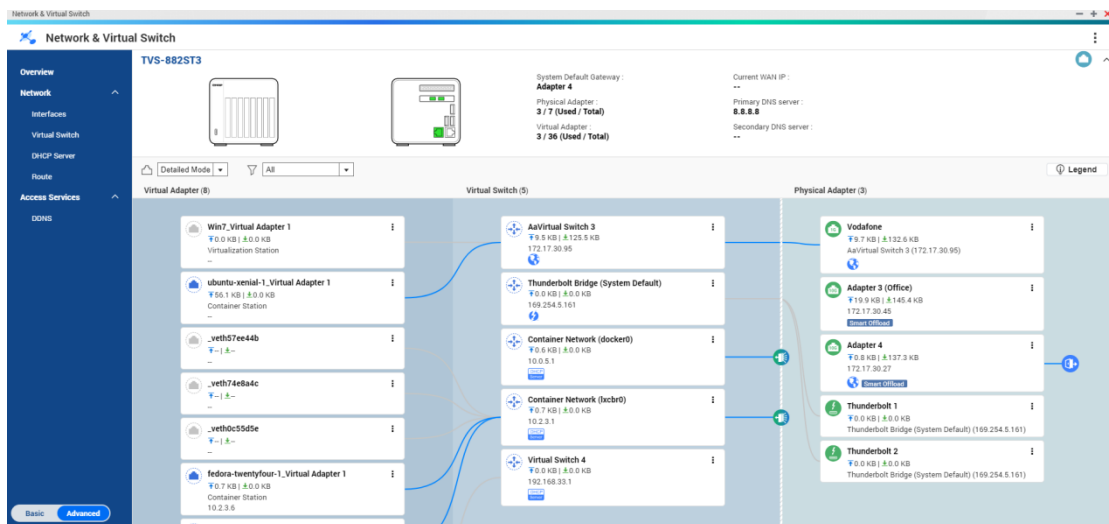
Basic and Advanced Mode

Network & Virtual Switch features two separate usage modes. Switch between these modes by clicking **Basic** or **Advanced** in the Network & Virtual Switch menu pane.

| Mode | Description |
|----------|--|
| Basic | <p>This mode is well-suited for most users, and requires minimal configuration of network settings.</p> <ul style="list-style-type: none"> Virtual Switch functions are disabled. Static Route functions are disabled. |
| Advanced | <p>This mode is best-suited for power-users who need more control over the configuration of network settings.</p> <ul style="list-style-type: none"> Virtual Switch functions are enabled. Static Route functions are enabled. |

Overview

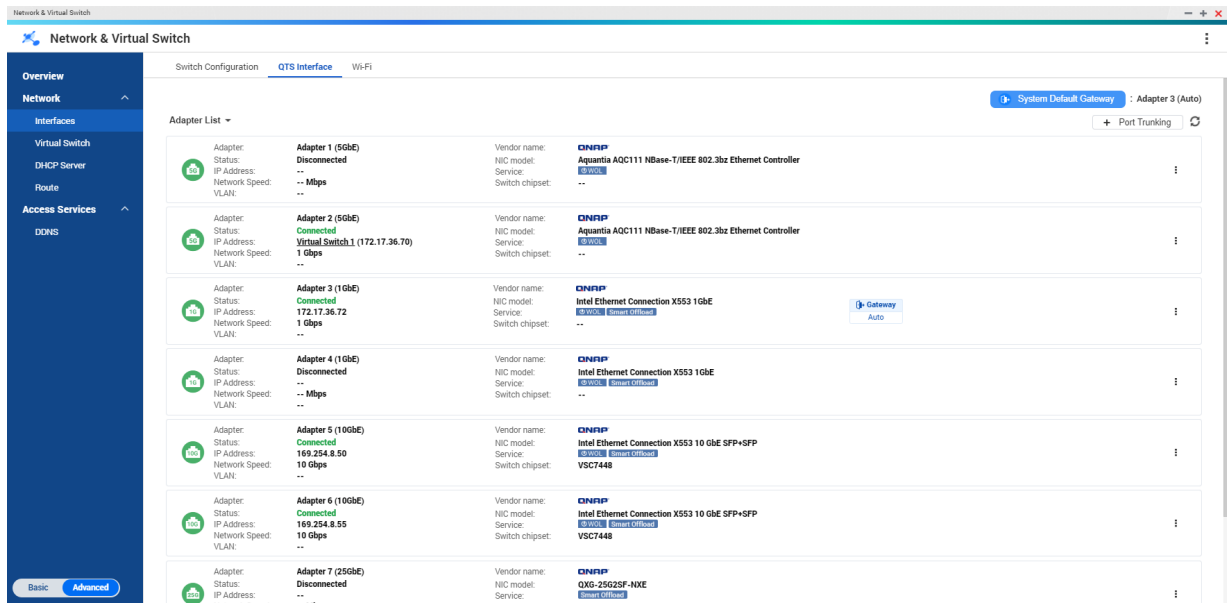
This screen provides a general overview of the network topology, IP address, status, and usage information for each device on the network.



Interfaces

This screen displays the physical adapter list as well as the physical adapter/SR-IOV topology when a Serial Root I/O Virtualization (SR-IOV) enabled network interface card (NIC) is connected to the device. The screen

provides access to basic network settings and allows the configuration of physical adapters. The Interface section allows you to configure settings related to IPv4, IPv6, DNS, port trunking, VLAN, Thunderbolt, USB QuickAccess, and Wi-Fi.






IP Address

Configuring IPv4 Settings


1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click **Configure** .
The **Configure** window opens.
4. Configure the IPv4 settings.

| Setting | Description |
|---|---|
| Obtain IP address settings automatically via DHCP | If the network supports DHCP, the adapter automatically obtains the IP address and network settings. |
| Use static IP address | Manually assign a static IP address. You must specify the following information: <ul style="list-style-type: none"> • Fixed IP Address • Subnet Mask • Default Gateway |




| Setting | Description |
|---------------|---|
| Jumbo Frame | <p>Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QTS supports the following MTU sizes:</p> <ul style="list-style-type: none"> • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes <p> Important</p> <ul style="list-style-type: none"> • All connected network devices must enable Jumbo Frames and use the same MTU size. • Only certain NAS models support Jumbo Frames. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster. |
| Network Speed | <p>Select the network transfer rate allowed by the network environment.</p> <p> Tip Selecting Auto-negotiation will automatically detect and set the transfer rate.</p> <p> Important The Network Speed field is automatically set to Auto-negotiation and hidden when configuring 10GbE & 40GbE adapters.</p> |

5. Click **Apply**.

Configuring IPv6 Settings

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure and then click  > **Configure** .
The **Configure** window opens.
4. Go to the **IPv6** tab.
5. Configure the IPv6 settings.

| Setting | Description |
|---------|--------------------------------|
| Disable | Do not assign an IPv6 address. |


| Setting | Description |
|-------------------------------------|--|
| IPv6 Auto-Configuration (Stateful) | <p>The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.</p> <p> Important This option requires an available DHCPv6-enabled server on the network.</p> |
| IPv6 Auto-Configuration (Stateless) | <p>The adapter automatically acquires an IPv6 address and DNS settings from the router.</p> <p> Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network.</p> |
| Use static IP address | <p>Manually assign a static IP address to the adapter. You must specify the following information:</p> <ul style="list-style-type: none"> • Fixed IP Address • Prefix length <p> Tip Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> • Default Gateway |

6. Click **Apply**.


DNS

A Domain Name System (DNS) server translates a domain name into an IP address.

Configuring DNS Settings

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
4. Go to the **DNS** tab.
5. Select one of the following options:

| Setting | Description |
|---|---|
| Obtain DNS server address automatically | Automatically obtain the IP address using DHCP. |

| Setting | Description |
|--------------------------------------|---|
| Use the following DNS server address | Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |

6. Click **Apply**.

Virtual LANs (VLANs)


A virtual LAN (VLAN) groups multiple network devices together and limits the broadcast domain. Members of a VLAN are isolated and network traffic is only sent between the group members. You can use VLANs to increase security and flexibility while also decreasing network latency and load.

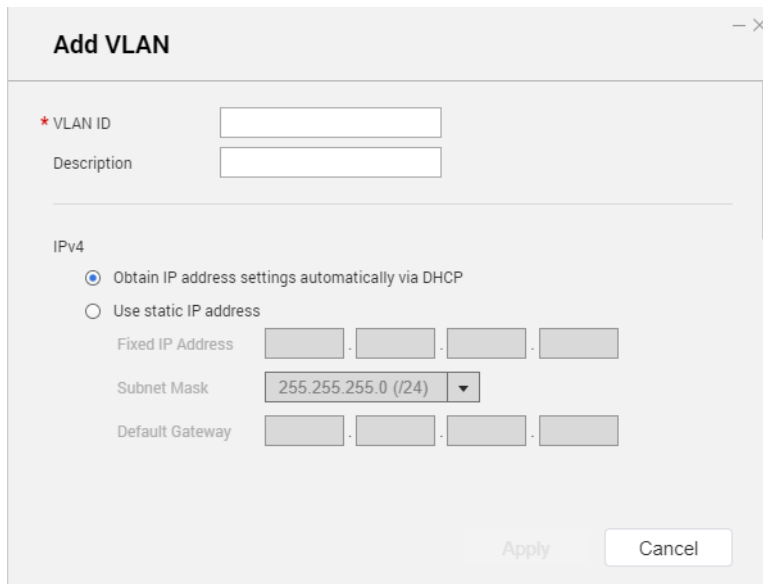
Adding an Interface to a VLAN



Important

When using both port trunking and a VLAN, port trunking must be configured first.

- Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
- Go to **Network > Interfaces** .
- Identify the adapter that you want to configure, then click  .
- Select **Add VLAN**.
The **Add VLAN** window opens.



- Specify a VLAN ID.

**Important**

The VLAN ID must be between 1 and 4094.

6. Specify a description for the VLAN.
7. Select one of the following options.

| Option | Steps |
|--|---|
| Automatically obtain the IP address using DHCP | Select Obtain IP address settings automatically via DHCP . |
| Use a static IP address | <ol style="list-style-type: none"> a. Select Use static IP address b. Specify a fixed IP address. c. Select a subnet mask. d. Specify the default gateway. |

8. Click **Apply**.

Port Trunking

Port trunking combines two or more Ethernet interfaces for increased bandwidth, load balancing and fault tolerance (failover). Load balancing is a feature that distributes workloads evenly across multiple Ethernet interfaces for higher redundancy. Failover ensures that a network connection remains available even if a port fails.

Configuring Port Trunking

**Important**

Before configuring Port Trunking, ensure at least two network interfaces are connected to the same switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Click **Port Trunking**.
The **Port Trunking** window opens.
4. Click **Add**.
The **Port Trunking (Add)** window opens.
5. Select two or more network interfaces to add to the trunking group.
6. Click **Next**.
7. Select a switch type.
8. Click **Next**.
9. Select a trunking mode.

**Important**

Some port trunking modes must be supported by your network switches. Selecting an unsupported mode may affect network performance or cause the network interface to freeze.

| Mode | Description |
|----------------------------|--|
| Fault Tolerance (Failover) | |
| Active-Backup | All traffic is sent and received using the interface that was first added to the trunking group. If this primary interface becomes unavailable, the secondary interface will become active. |
| Broadcast | Transmits the same network packets to all the network interface cards. |
| Load balancing & Failover | |
| Balance-tlb | Incoming traffic is received by the current interface. If the interface fails, a slave interface takes over the MAC address of the failed interface. Outgoing traffic is distributed based on the current load for each interface relative to the interface's maximum speed. |
| Balance-alb | Similar to Balance-tlb, but offers additional load balancing for incoming IPv4 traffic. |
| Balance-rr | Transmits network packets sequentially to each network interface card in order to distribute the internet traffic among all the NICs. |
| Balance-xor | Transmits network packets using the Hash algorithm, which selects the same NIC slave for each destination MAC address. |
| 802.3ad dynamic | Uses a complex algorithm to aggregate NICs and configure speed and duplex settings. |


10. Click **Apply**.

System Default Gateway

The system default gateway serves as the network access point for the NAS. By default, all external network traffic will pass through the gateway. A network interface must be specified for the default gateway.

Configuring the System Default Gateway

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Click **System Default Gateway**.
The **System Default Gateway** window opens.
4. Configure the system default gateway.

| Setting | Description |
|------------------------------------|--|
| Auto-select system default gateway | QTS automatically detects all adapter, virtual switch, PPPoE, and VPN connections that can be used to connect to the internet. It selects one of these connections and then sets it as the default gateway. |
| Select the system default gateway | Manually assign an adapter to serve as the system default gateway. Optionally, set a backup failover gateway. The failover default gateway field is only available when multiple interfaces are connected. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Tip When assigning a PPPoE or VPN connection as the default gateway, ensure a stable physical connection is also set as the failover default gateway.</p> </div> </div> |

5. Optional: Disable the NCSI service.

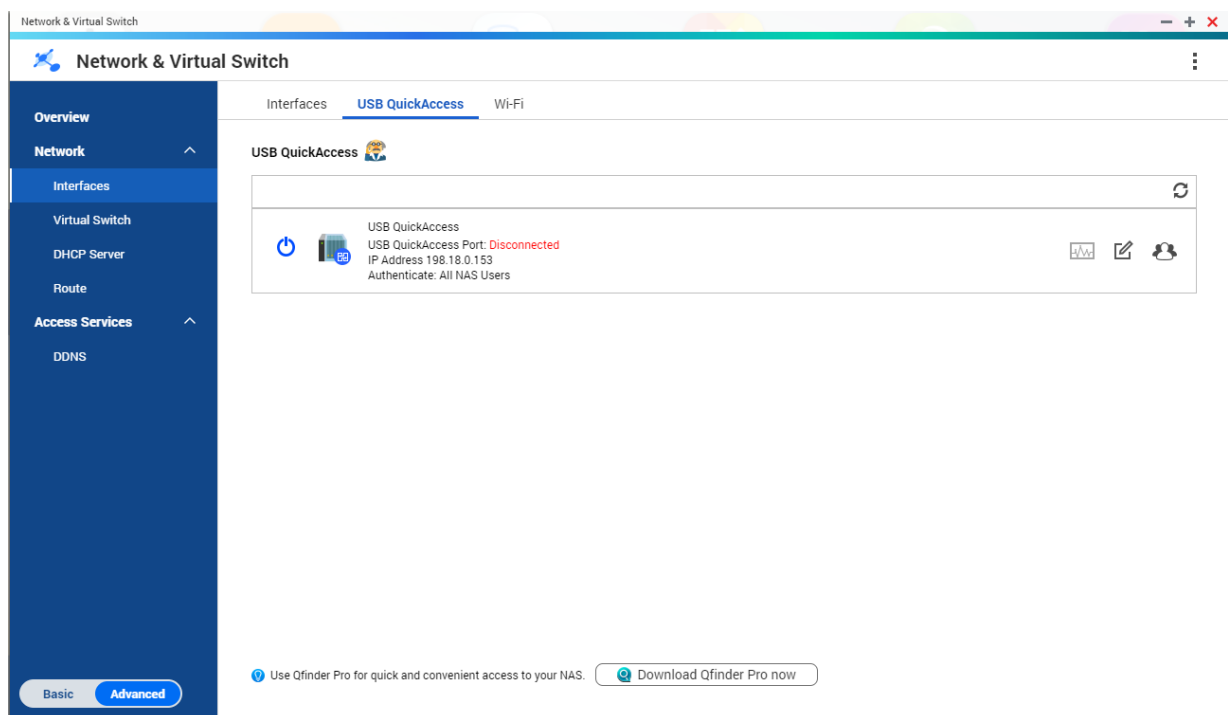
**Tip**

The QTS Network Connectivity Status Indicator (NCSI) periodically performs tests to check the speed and status of NAS network connections.

6. Click **Apply**.


USB QuickAccess

This screen controls the configuration and management of USB QuickAccess services on the NAS. USB QuickAccess allows a computer to connect to the NAS using a USB cable and the Common Internet File System (CIFS).



**Tip**

- USB QuickAccess is only available on certain models.
- It is not possible to configure, delete, or disable DHCP servers created with USB QuickAccess.



Enabling USB QuickAccess


1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4. Click  .

Configuring the USB QuickAccess IP address

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4.  Click  .
The **Configure** window opens.
5. Enter a static IP Address.
6. Click **Apply**.

Configuring USB QuickAccess Authentication

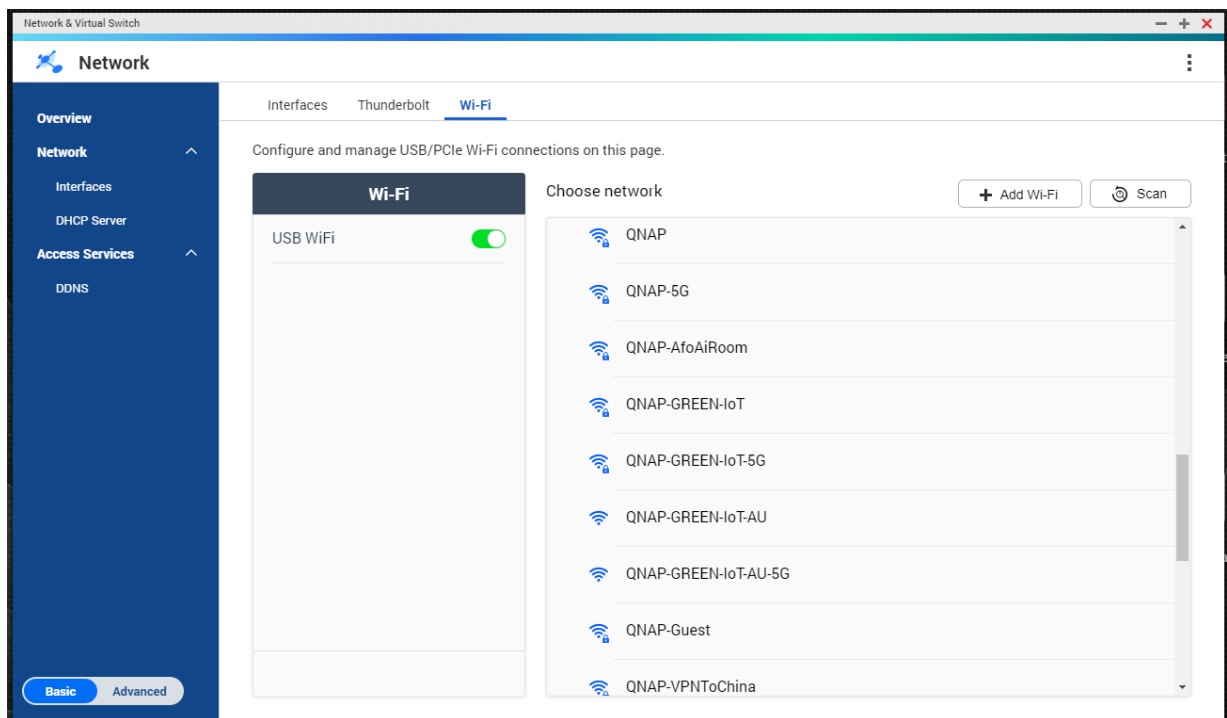
1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4.  Click  .
The **Configuration** window opens.
5. Select an authentication method:

| Authentication Method | Description |
|-----------------------|--|
| All NAS Users | A QTS username and password is required to access files. |
| Everyone | No username or password is required to access files. |
| Selected Users/Groups | Administrators can grant access to specific QTS users or groups. A QTS username and password is required to access files. <div style="display: flex; align-items: flex-start;">  <div> <p>Tip To grant access to domain users, first set up Domain Security. Go to Control Panel > Privilege > Domain Security .</p> </div> </div> |

6. Click **Apply**.

Wi-Fi


This screen controls the configuration and management of Wi-Fi connections accessible from the NAS.



Important

- A USB or PCIe Wi-Fi device must be installed to access these features.
 - For a list of compatible USB Wi-Fi dongles, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > USB Wi-Fi**.
 - For a list of compatible PCIe Wi-Fi cards, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > Expansion Card > QNAP**.
- QTS supports the simultaneous use of multiple PCIe Wi-Fi cards, but only one USB Wi-Fi dongle can be in used at a time.





Enabling Wi-Fi

1. Go to **Control Panel > Network & Virtual Switch**.
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces**.
3. Go to the **Wi-Fi** tab.
4. Click .

Connecting to a Wireless Network



1. Go to **Control Panel > Network & Virtual Switch**.
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces**.

3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible networks.
5. Select a wireless network from the list.

| Icon | Description |
|---|--|
|  | The Wi-Fi network requires a password. |
|  | Connect to a Wi-Fi network without a password. |
|  | <ul style="list-style-type: none"> • The Wi-Fi connection cannot access the internet. • The Wi-Fi connection requires an additional login. <p> Tip QTS does not support networks that require an additional login.</p> |

The settings panel expands.

6. Click **Connect**.
7. Optional: Configure connection settings.

| Setting | Description |
|------------------------|--|
| Password | Enter the password provided by the network administrator.  Tip Click  to make the password visible. |
| Connect automatically | Automatically connect to this network whenever it is in range. |
| Connect even if hidden | Attempt to connect to this network even if the SSID is hidden. |

8. Click **Apply**

Connecting to a Captive-Portal-Enabled Wireless Network Using Browser Station

Captive portal allows organizations to easily share their network environment with customers, employees, and other guests.

QTS supports the captive portal function that connects to the internet through an access point in the wireless network.

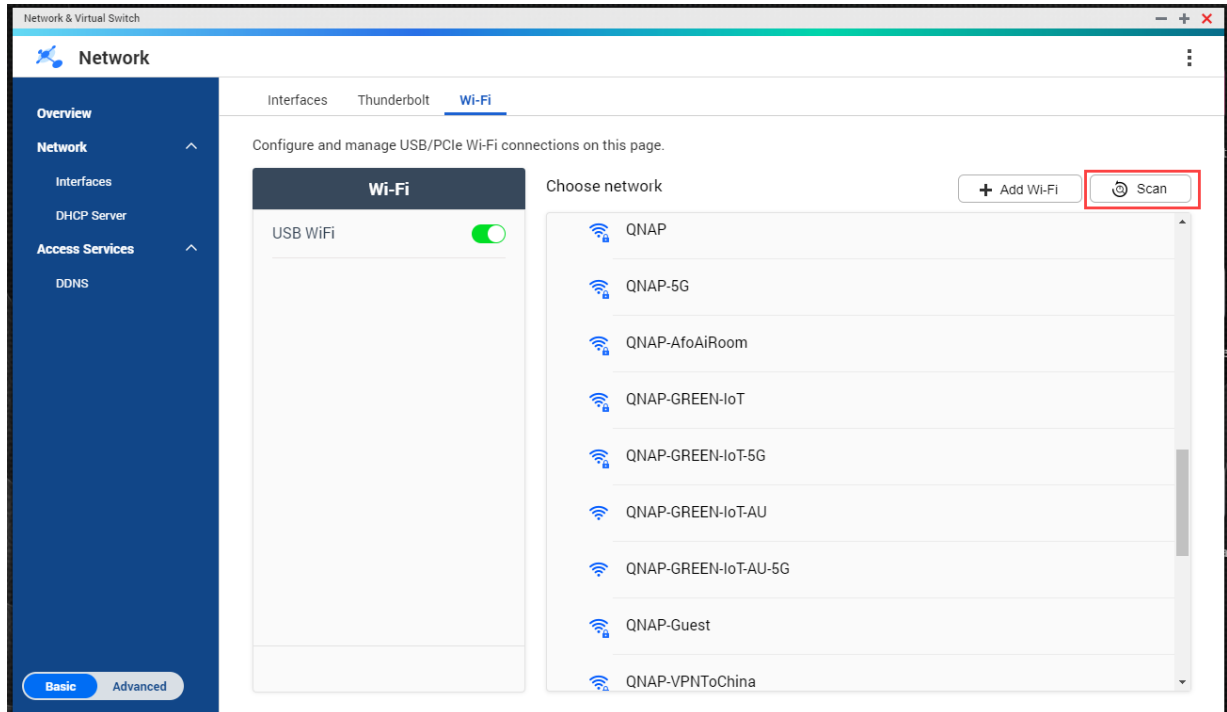


Note

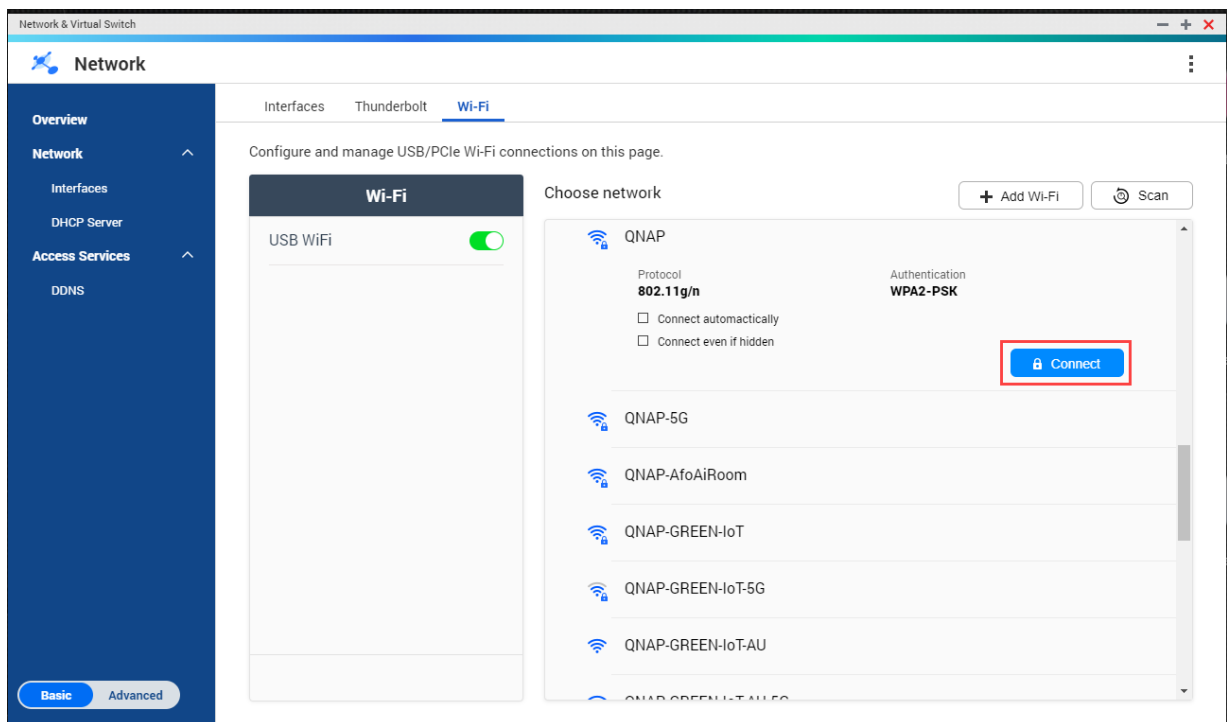
Download and install Browser Station from App Center to access the captive portal functions.
Alternatively, QNAP recommends installing Qfinder Pro(6.9.2 or later) to utilize the captive portal function on a wireless network.
For details, see [Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro](#).

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.

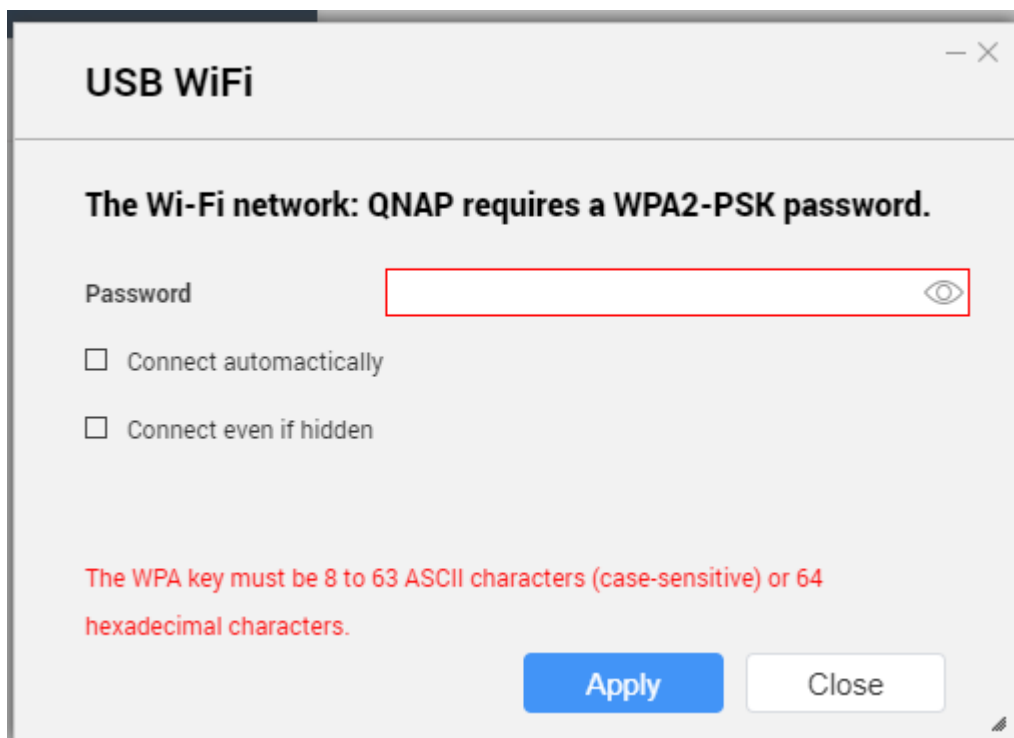
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible wireless networks enabled with captive portal.



5. Select the captive-portal-enabled wireless network from the list.
The settings panel expands.
6. Click **Connect**.



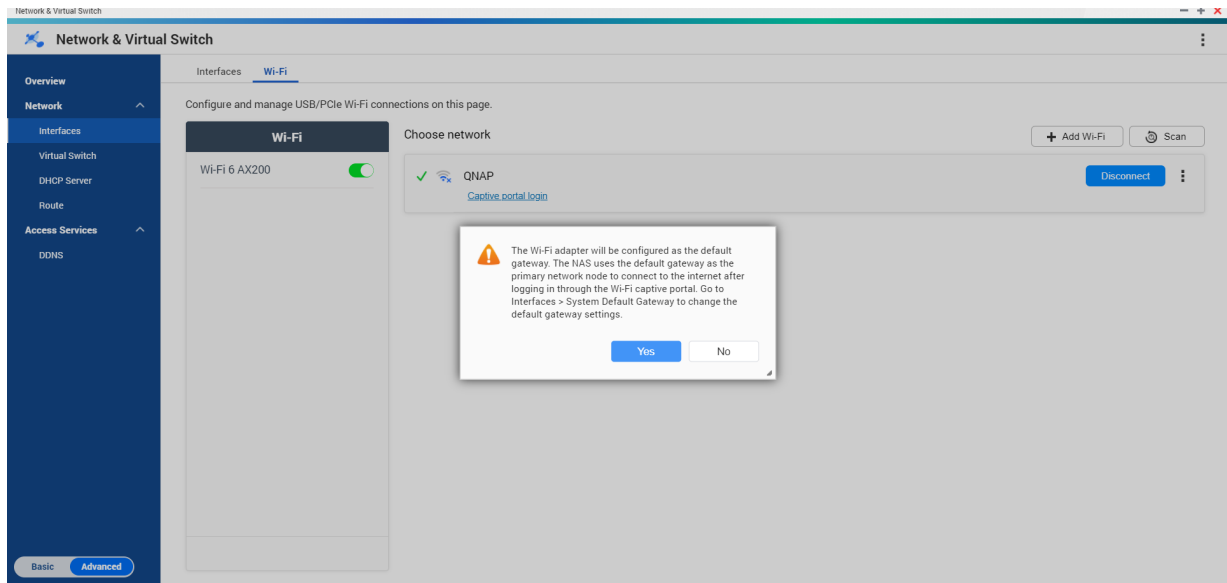
7. Optional: Configure connection settings.



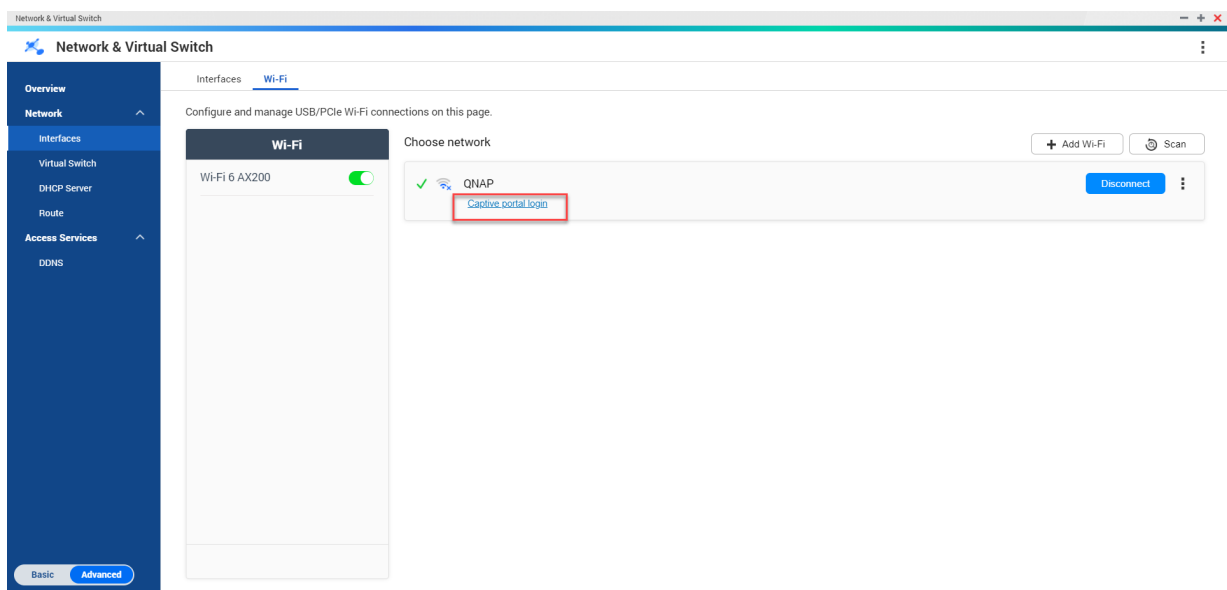
For configuration details and wireless icon descriptions, see [Connecting to a Wireless Network](#).

8. Click **Apply**.

A pop-up window opens specifying the change in the default network gateway.



9. Click **Yes**.
10. Optional: Go to **Interfaces > System Default Gateway** to change the default network gateway settings.
11. Click **Captive portal login**.



Browser Station automatically redirects you to the captive portal landing page.

12. Enter the username and password to connect to the wireless network.

Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro




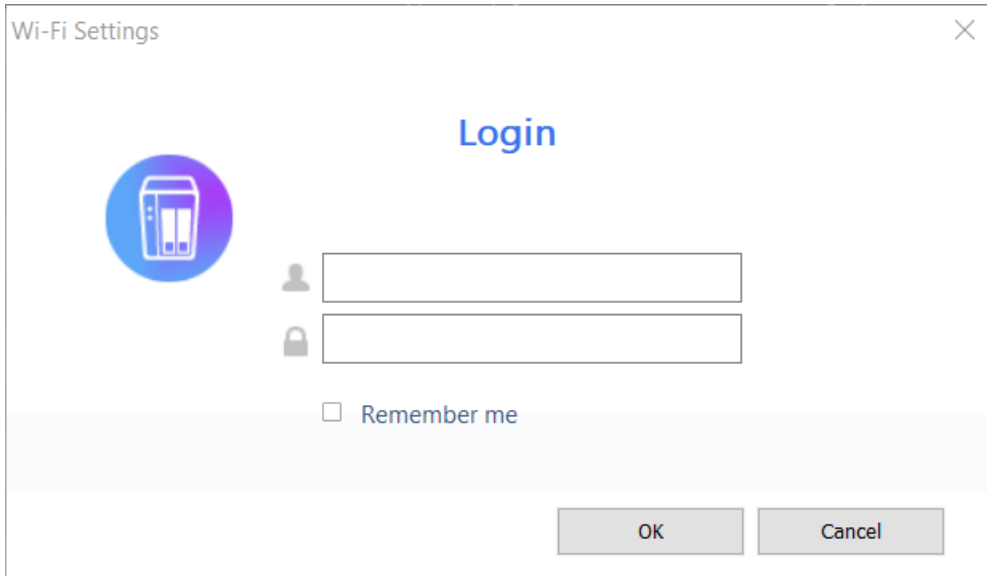
Note

QNAP recommends installing Qfinder Pro (Windows 6.9.2 or later and MacOS/Linux 7.3.2 or later) to utilize the captive portal function on a wireless network.

**Important**

Connect the NAS directly to the PC using an ethernet cable in order to connect to a wireless network enabled with captive portal.

1. Open Qfinder Pro.
2. Locate the NAS in the list and click the unconfigured Wi-Fi icon  located under the Status table header.
3. Optional: Alternatively, select the NAS and go to **Settings > Wi-Fi Settings** . The **Login** page opens.



Wi-Fi Settings

Login

Remember me

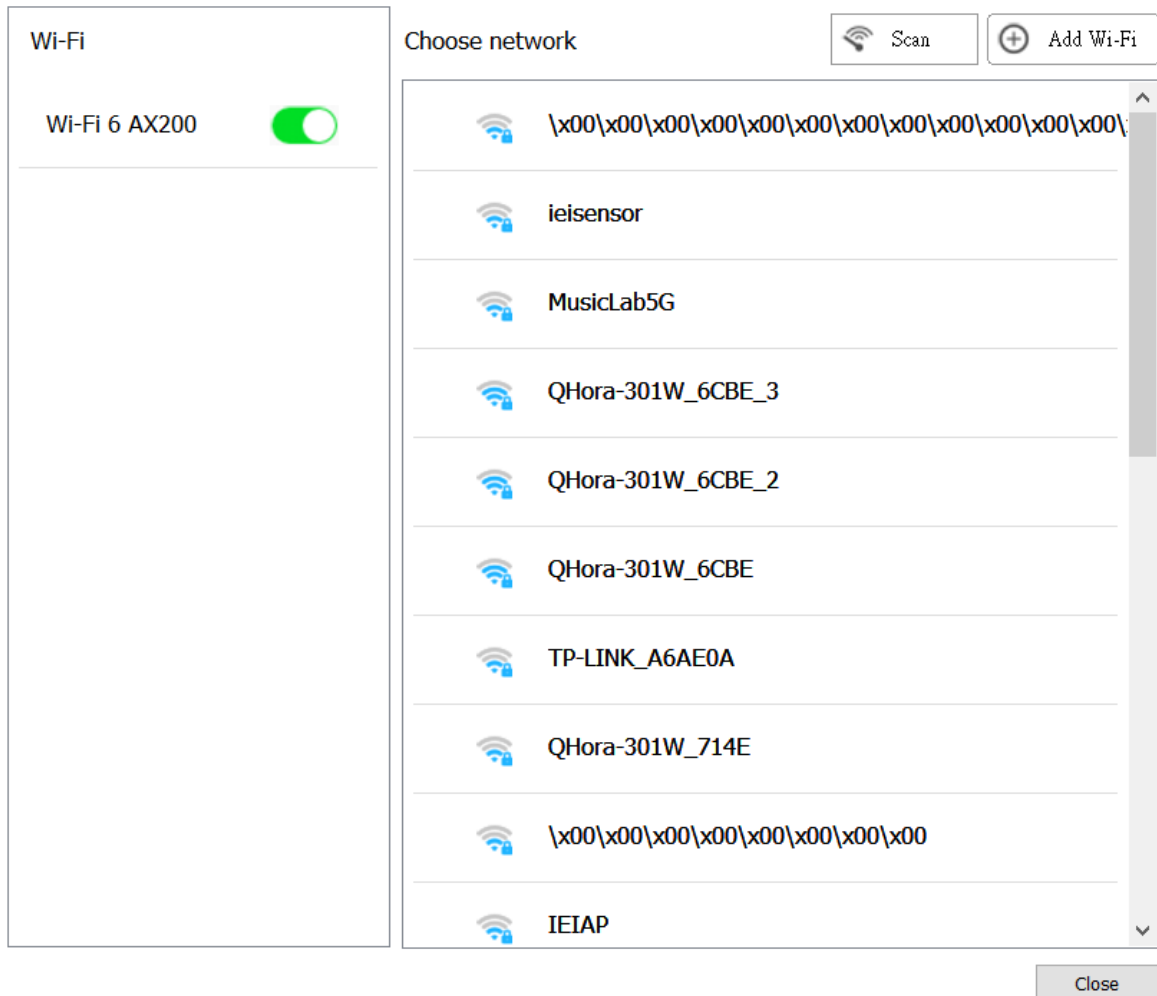
OK Cancel

4. Enter the username and password.
5. Click **OK**.
The **Wi-Fi Connection Settings** page opens.

Wi-Fi Connection Settings



You can manage and configure Wi-Fi connection settings here.

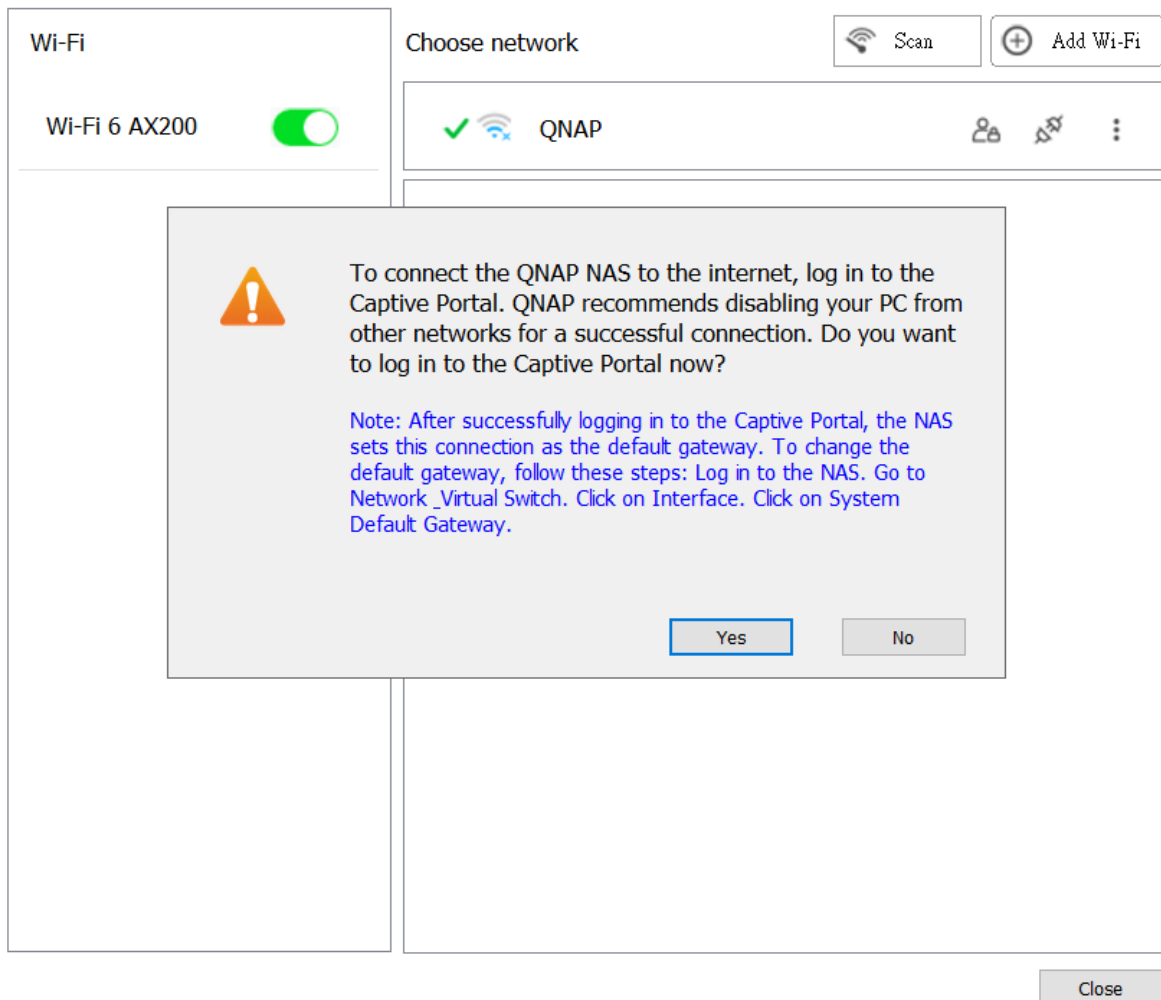


6. Select the wireless network from the list.
The settings panel expands.
7. Click **Connect**.
8. Configure connection settings.
9. Click **Apply**.
A pop-up window opens.

Wi-Fi Connection Settings



You can manage and configure Wi-Fi connection settings here.



10. Click **Yes.**


The default browser automatically opens and redirects you to the captive portal landing page.



Note

Network & Virtual Switch automatically enables NAT and DHCP on the Wi-Fi adapter in the background.



11. Enter the username and password to connect to the wireless network.

Qfinder Pro displays the wireless connection icon  in the Qfinder Pro NAS status panel.


Adding a Wireless Network



1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.

4. Click **Add Wi-Fi**.
The **Connect to a Wi-Fi network** window opens.
5. Configure connection settings.

| Setting | Description |
|--------------------------------|---|
| Network Name | Enter the name of the wireless network. |
| Security Type | <p>Select the encryption used by the wireless network.</p> <ul style="list-style-type: none"> • No Authentication (Open): Any wireless device can connect to the network. This is the default setting. • WEP: Use Wired Equivalent Privacy (WEP) if the wireless device does not support WPA or WPA2. • WPA- Personal: Use Wi-Fi Protected Access (WPA)- Personal as an intermediate security measure if the wireless device does not support WPA2. • WPA2-Personal: Uses Advanced Security Encryption (AES) for data encryption. This is the suggested security mechanism if the wireless device supports WPA2. • WPA- & WPA2- Enterprise: Use this security mechanism if the wireless device supports transition from WPA-Enterprise to WPA2-Enterprise. The network automatically chooses the encryption method used by the wireless device. |
| Password | <p>Enter the password provided by the network administrator.</p> <p> Tip Click  to make the password visible.</p> |
| Automatically connect when the | Automatically connect to this network whenever it is in range. |
| Connect even if hidden | Attempt to connect to this network even if the SSID is hidden. |

6. Optional: Configure WPA- & WPA2 Enterprise settings.

| Setting | Description |
|---------------------------------|--|
| Authentication | <p>Authentication is specific to WPA- and WPA2- Enterprise encryption. You can select a method based on the authentication supported by your device.</p> <ul style="list-style-type: none"> • Protected EAP (PEAP): Protected Extensible Authentication Protocol (PEAP) provides a more secure authentication to 802.11 WLANs. • EAP-TTLS: EAP Tunneled Transport Layer Security (EAP-TTLS) supports legacy authentication mechanisms. |
| Certificate Authority (CA) File | <p>A data file that contains identification credentials to help authenticate the WPA-WPA2 public key ownership.</p> <p> Note Select CA file is not required if you do not have access to a digital certificate.</p> |

| Setting | Description |
|----------------------|--|
| Inner Authentication | <p>Select an inner authentication method based on PEAP or EAP-TTLS authentication.</p> <p>MS-CHAPv2 is the default inner authentication method for PEAP. The following inner authentication methods are available if the authentication method is set to EAP-TTLS:</p> <ul style="list-style-type: none"> • PAP • CHAP • MS-CHAP • MS-CHAPv2 |
| Username | Enter the username provided by the network administrator. |
| Password | <p>Enter the password provided by the network administrator.</p> <p> Tip Click  to make the password visible.</p> |

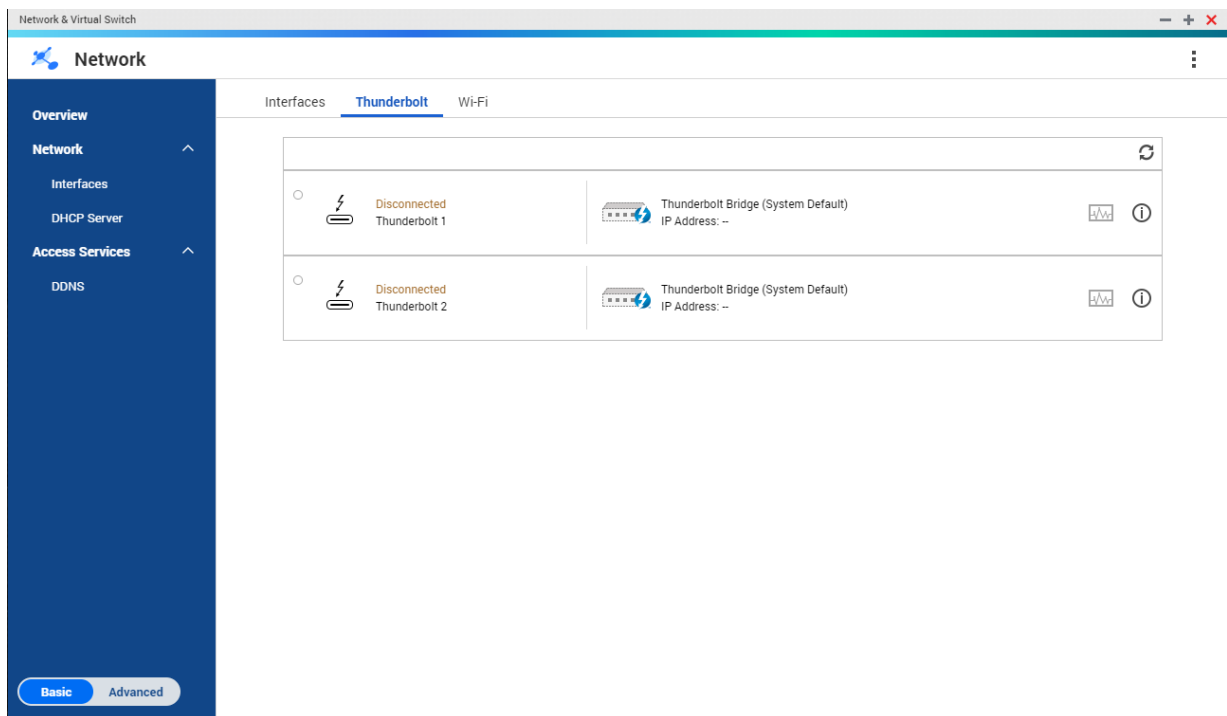
7. Click **Connect**.

Connection Messages

| Message | Description |
|-----------------------------|--|
| Connected | The NAS is currently connected to the Wi-Fi network. |
| Connecting | The NAS is trying to connect to the Wi-Fi network. |
| Out of range or hidden SSID | The wireless signal is not available or the SSID is not being broadcast. |
| Failed to get IP | The NAS is connected to the Wi-Fi network but could not get an IP address from the DHCP server. Check the router settings. |
| Association failed | The NAS cannot connect to the Wi-Fi network. Check the router settings. |
| Incorrect key | The entered password is incorrect. |
| Auto connect | Automatically connect to the Wi-Fi network. This is not supported if the SSID of the Wi-Fi network is hidden. |

Thunderbolt

This screen displays port and connection information related to any Thunderbolt interfaces on the NAS.



Thunderbolt to Ethernet (T2E)

Thunderbolt to Ethernet functionality allows the Thunderbolt port to act as an Ethernet interface.



Tip

QNAP recommends using Qfinder Pro when configuring Thunderbolt to Ethernet.



Important

Due to Thunderbolt driver issues, T2E connections using Thunderbolt port 2 may have connectivity problems when connecting to Windows. Thunderbolt port 3 connections are unaffected.

Enabling T2E with Qfinder Pro

Qfinder Pro is a utility for Windows, Mac, and Linux that allows you to quickly find and access a QNAP NAS over a LAN.

For the current version of Qfinder Pro, please visit <https://www.qnap.com/utilities>.



Tip

Qfinder Pro automatically configures the `/etc/sysctl.conf` settings file on macOS.

1. Open **Qfinder Pro**.
2. Locate the NAS using **Qfinder Pro**.
3. Click the Thunderbolt icon.
The T2E window opens.
4. Select **Enable T2E**.
5. Click **Apply**.

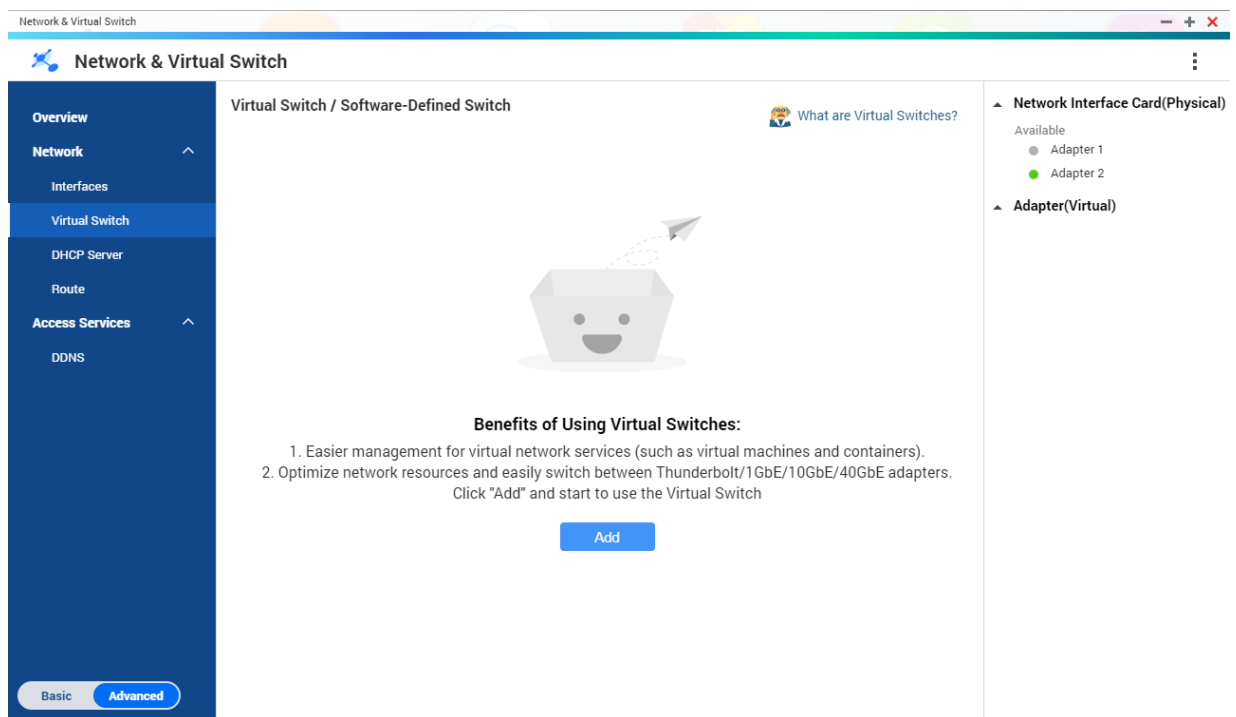
Enabling T2E on macOS

1. Open the Terminal.
2. Run the command.

| Command | Notes |
|--|---|
| <code>sudo sysctl net.inet.tcp.path_mtu_discovery=0 && sudo sysctl net.inet.tcp.tso=0</code> | This command will only temporarily enable T2E. Restarting the Mac will delete the connection. |
| <code>sudo bash -c 'printf "#QNAP\nnet.inet.tcp.path_mtu_discovery=0\nnet.inet.tcp.tso=0\n#QNAP\n" >> /etc/sysctl.conf'</code> | This command will permanently apply these settings. |


Virtual Switches

This screen controls the configuration and management of virtual switches running on the NAS. Virtual Switches allow physical interfaces and virtual adapters to communicate with each other.



QTS supports three different virtual switch modes.

| Mode | Description |
|----------|--|
| Basic | This mode is well-suited for most users, and requires minimal configuration of network settings. |
| Advanced | This mode is best-suited for power-users who need more control over the configuration of network settings. |

| Mode | Description |
|-------------------------|--|
| Software-Defined Switch | <p>This mode is suited for power-users who need to simulate an L2 physical switch.</p> <p> Important Packet forwarding rates are limited when using this mode.</p> |

**Tip**

To access this page, Network & Virtual Switch must be operating in [Advanced Mode](#).

Creating a Virtual Switch in Basic Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Basic Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Apply**.



Creating a Virtual Switch in Advanced Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Advanced Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Next**.
8. Configure the virtual switch IP address.

| Address Type | Description |
|----------------------------|--|
| DHCP Client | Assigns a dynamic IP address to the virtual switch. |
| Static IP | Assigns a static IP address to the virtual switch.  Tip Examine your network setup for guidance on how to best configure these settings. |
| Do not assign IP Addresses | Does not assign an IP address to the virtual switch after creation.  Tip This setting should be used when creating a virtual switch for special purposes, such as when building an external or isolated network. |

9. Click **Next**.

10. Configure the virtual switch services.

a. Enable the NAT service.



Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- The IP address of the virtual switch cannot be in a reserved range that doesn't support forwarding:
 - 127.xxx.xxx.xxx
 - 169.254.xxx.xxx
 - 192.0.2.xxx
 - 198.51.100.xxx
 - 203.0.113.xxx






b. Optional: Enable the DHCP Server.



Important



- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- To avoid IP address conflicts, do not enable DHCP server if there is another DHCP server running on the local network.


| Setting | Description |
|------------------|--|
| Start IP Address | Specify the starting IP address in a range allocated to DHCP clients. |
| End IP Address | Specify the ending IP addresses in a range allocated to DHCP clients. |
| Subnet Mask | Specify the subnet mask used to subdivide your IP address. |
| Lease Time | Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires. |

| Setting | Description |
|----------------------|---|
| Default Gateway | Specify the IP address of the default gateway for the DHCP server. |
| Primary DNS Server | Specify a DNS server for the DHCP server. |
| Secondary DNS Server | Specify a secondary DNS server for the DHCP server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |
| WINS Server | Specify the WINS server IP address.  Tip Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. |
| DNS Suffix | Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names. |
| TFTP Server | Specify the public IP address for the TFTP server.  Tip QTS supports both PXE and remote booting of devices |
| Boot File | Specify location and file name of the TFTP server boot file.  Tip QTS supports both PXE and remote booting of devices |

11. Click **Next**.


12. Configure the virtual switch IPv6 address.

| Setting | Description |
|-------------------------------------|--|
| Disable | Do not assign an IPv6 address. |
| IPv6 Auto-Configuration (Stateful) | The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.  Important This option requires an available DHCPv6-enabled server on the network. |
| IPv6 Auto-Configuration (Stateless) | The adapter automatically acquires an IPv6 address and DNS settings from the router.  Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network. |

| Setting | Description |
|-----------------------|---|
| Use static IP address | <p>Manually assign a static IP address. You must specify the following information:</p> <ul style="list-style-type: none"> • Fixed IP Address • Prefix length <p> Tip Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> • Default Gateway |

13. Click **Next**.

14. Configure the DNS settings.

| Setting | Description |
|---|---|
| Obtain DNS server address automatically | Automatically obtain the DNS server address using DHCP. |
| Use the following DNS server address | <p>Manually assign the IP address for the primary and secondary DNS servers.</p> <p> Important QNAP recommends specifying at least one DNS server to allow URL lookups.</p> |

15. Click **Next**.

16. Confirm the virtual switch settings.

17. Click **Apply**.

Creating a Virtual Switch in Software-defined Switch Mode



Important

To avoid bridge loops, please ensure any Ethernet cables are connected to the same switch before configuring a Software-defined Switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.
The **Create a Virtual Switch** window opens.
4. Select **Software-defined Switch Mode**.
5. Select one or more adapters.
6. Optional: Select **Enable the Spanning Tree Protocol**.



Tip

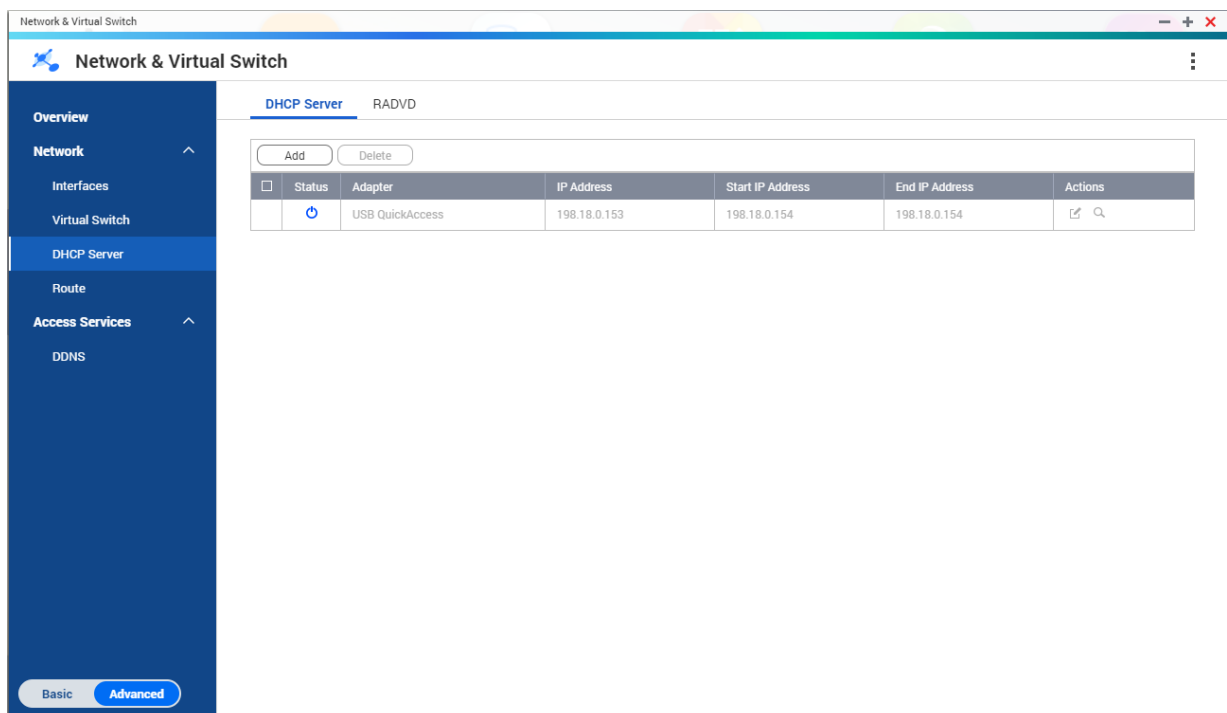
Enabling this setting prevents bridge loops.

7. Click **Apply**.

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) allows devices in a TCP/UDP network to be automatically configured for the network as the device is booted. The DHCP service uses a client-server mechanism, wherein a DHCP server stores and manages network configuration information for clients and offers necessary data when a client requests the information. The information includes the IP address and subnet mask, the IP address of the default gateway, the DNS server IP address, and the IP lease information.

This screen controls the creation and management of DHCP servers. DHCP servers can assign IPv4 addresses to clients on the network, while RADVD servers assign IPv6 addresses.



Important

Do not create a new DHCP server if one already exists on the network. Enabling multiple DHCP servers on the same network can cause IP address conflicts or network access errors.

Creating a DHCP Server

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Click **Add**.
The **DHCP Server** window opens.
4. Select an interface.
5. Click **Next**.

6. Select the network environment for the DHCP server.

| Option | Description |
|---|--|
| Enable DHCP server on the current network. | <ul style="list-style-type: none"> The adapter keeps the existing IP address and subnet mask. The DHCP server shares the subnet mask with the adapter and is assigned the next available IP address. |
| Reassign an IP address to the adapter and enable a DHCP server on a new subnet. | <ul style="list-style-type: none"> The adapter is assigned a new IP address and subnet mask. The DHCP server uses a different subnet mask and IP address. |
| Enable DHCP server for another subnet. | <ul style="list-style-type: none"> The adapter keeps the existing IP address and subnet mask. The DHCP server uses a different subnet mask and IP address. |

7. Click **Next**.

8. Configure a static IP address for the adapter.





Important

A static IP address must be configured when creating a DHCP server.





- a. Click **Yes**.
- b. Configure IP address settings.


| Setting | Description |
|------------------|--|
| Fixed IP Address | <p>Specify a fixed IP address.</p> <div style="display: flex; align-items: center;"> <p>Tip Examine your network setup for guidance on how to best configure these settings.</p> </div> |
| Subnet Mask | Specify the subnet mask used to subdivide your IP address. |
| Default Gateway | Specify the IP address of the default gateway for the adapter. |
| Jumbo Frame | <p>Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QTS supports the following Jumbo Frame sizes:</p> <ul style="list-style-type: none"> 1500 bytes (default) 4074 bytes 7418 bytes 9000 bytes <div style="display: flex; align-items: center;"> <p>Important</p> <ul style="list-style-type: none"> Jumbo Frames are only supported by certain NAS models. Using Jumbo Frames requires a network speed of 1000 Mbps or faster. All connected network devices must enable Jumbo Frames and use the same MTU size. </div> |

| Setting | Description |
|----------------------|--|
| Network Speed | Specify the speed at which the adapter will operate.  Tip Auto-negotiation will automatically detect and set the transfer rate. |
| Primary DNS Server | Assign an IP address for the primary DNS server. |
| Secondary DNS server | Assign an IP address for the secondary DNS server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |

c. Click **Next**.

9. Configure DHCP settings.

| Setting | Description |
|----------------------|--|
| Start IP Address | Specify the starting IP address in a range allocated to DHCP clients. |
| End IP Address | Specify the ending IP addresses in a range allocated to DHCP clients. |
| Subnet Mask | Specify the subnet mask used to subdivide your IP address. |
| Lease Time | Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires. |
| Default Gateway | Specify the IP address of the default gateway for the DHCP server. |
| Primary DNS Server | Specify a DNS server for the DHCP server. |
| Secondary DNS Server | Specify a secondary DNS server for the DHCP server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |
| WINS Server | Specify the WINS server IP address.  Tip Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. |
| DNS Suffix | Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names. |
| TFTP Server | Specify the public IP address for the TFTP server.  Tip QTS supports both PXE and remote booting of devices. |

| Setting | Description |
|-----------|--|
| Boot File | <p>Specify location and file name of the TFTP server boot file.</p> <p> Tip QTS supports both PXE and remote booting of devices.</p> |

10. Click **Apply**.

DHCP Clients

A DHCP client is a network device using DHCP service to obtain network configuration parameters such as an IP address from a DHCP server. When a DHCP client sends a broadcast message to locate a DHCP server, the DHCP server provides configuration parameters (IP address, MAC address, domain name, and a lease for the IP address) to the client.

Physical Adapter DHCP Client

Enabling a DHCP IPv4 address allows the device to automatically acquire an IPv4 address for a specific physical adapter from a DHCP server. The physical adapter is assigned an IP address by the DHCP server for a predefined lease time.



Note

For details on obtaining a DHCP provided IP address, see [Configuring IPv4 Settings](#).

Virtual Switch DHCP Client

Virtual switches allow virtual machines to obtain IP-related configurations automatically from an external DHCP server. The virtual switch obtains the IP address from the DHCP server through the connected physical adapter on the device.

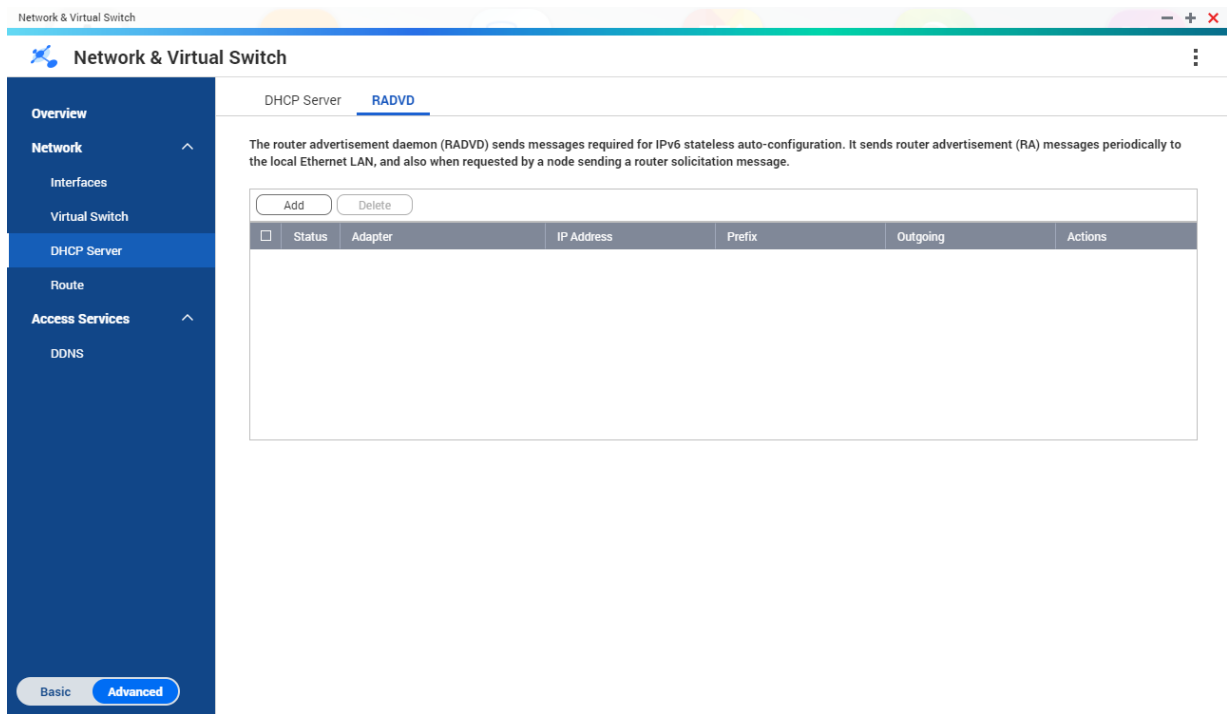


Note

1. A virtual switch configured with an automatic DHCP IP address cannot utilize the NAT and DHCP server functions.
2. Virtual switches cannot automatically acquire the IP address of the physical adapter unless the virtual switch has been configured to connect to a physical adapter in **Virtual Switch > Basic Mode/Advanced Mode**.

RADVD

This screen controls the creation and management of Router Advertisement Daemon (RADVD) servers. This service sends messages required for IPv6 stateless auto-configuration. This service periodically sends router advertisement (RA) messages to devices on the local network, and can also send a router solicitation messages when requested from a connected node.



Creating an RADVD Server


1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Go to the **RADVD** tab.
4. Click **Add**.
The **RADVD - Outgoing Interface** window opens.
5. Select the outgoing interface.
6. Click **Next**.
7. Configure a static IP address for the adapter.





Important

A static IP address must be configured when creating a RADVD server.

- a. Click **Yes**.
- b. Optional: Configure Static IP address settings.

| Setting | Description |
|------------------|---|
| Fixed IP Address | Specify a fixed IP address.  Tip Examine your network setup for guidance on how to best configure these settings. |

| Setting | Description |
|----------------------|--|
| Prefix Length | Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP. |
| Default Gateway | Specify the IP address of the default gateway for the DHCP server. |
| Primary DNS Server | Assign an IP address for the primary DNS server. |
| Secondary DNS server | Assign an IP address for the secondary DNS server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |

c. Click **Next**.

8. Select a second adapter for the RADVD service interface.

9. Click **Next**.

10. Optional: Configure a static IP address for the second RADVD adapter.






Important

Creating an RADVD interface requires that the adapter use a static IP address. If the adapter already uses a static IP address, skip this step.




a. Click **Yes**.

b. Configure Static IP address settings.

| Setting | Description |
|----------------------|---|
| Fixed IP Address | Specify a fixed IP address.  Tip Examine your network setup for guidance on how to best configure these settings. |
| Prefix Length | Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP. |
| Default Gateway | Specify the IP address of the default gateway for the adapter. |
| Primary DNS Server | Specify the DNS server address. |
| Secondary DNS server | Specify the DNS server address.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |

c. Click **Apply**.

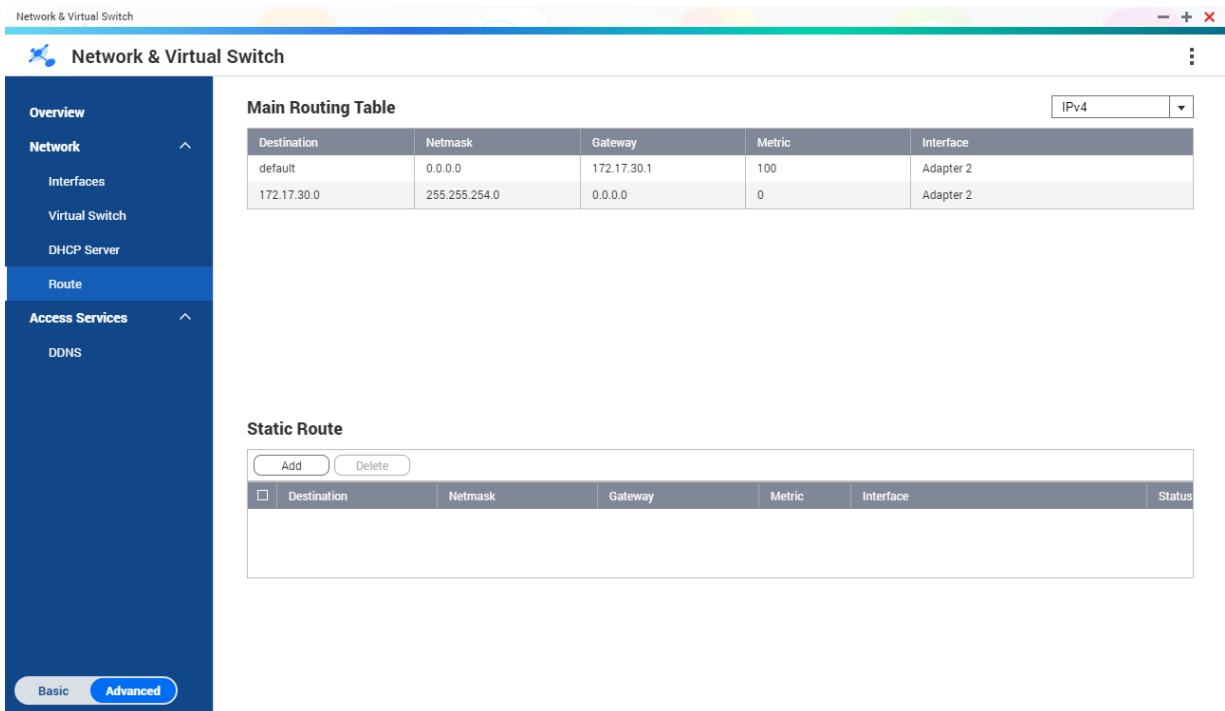
11. Configure the RADVD server settings.

| Setting | Description |
|----------------------|---|
| Prefix | Specify the routing prefix for the adapter.  Tip Examine your network setup for guidance on how to best configure these settings. |
| Prefix Length | Specify the prefix length for the adapter.  Tip Obtain the prefix and the prefix length information from your ISP. |
| Lease Time | Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires. |
| Primary DNS Server | Specify the DNS server address. |
| Secondary DNS server | Specify the DNS server address.  Important QNAP recommends specifying at least one DNS server to allow URL lookups. |

12. Click **Apply**.

Route

This screen controls the creation of static routes. Under normal circumstances, QTS automatically obtains routing information after it has been configured for Internet access. Static routes are only required in special circumstances, such as having multiple IP subnets located on your network.



The screenshot shows the 'Network & Virtual Switch' configuration page in QTS. The left sidebar contains a navigation menu with 'Route' selected. The main content area is divided into two sections: 'Main Routing Table' and 'Static Route'.

Main Routing Table (IPv4):

| Destination | Netmask | Gateway | Metric | Interface |
|-------------|---------------|-------------|--------|-----------|
| default | 0.0.0.0 | 172.17.30.1 | 100 | Adapter 2 |
| 172.17.30.0 | 255.255.254.0 | 0.0.0.0 | 0 | Adapter 2 |

Static Route


Buttons: Add, Delete

| <input type="checkbox"/> | Destination | Netmask | Gateway | Metric | Interface | Status |
|--------------------------|-------------|---------|---------|--------|-----------|--------|
| | | | | | | |

At the bottom of the sidebar, there are 'Basic' and 'Advanced' tabs, with 'Advanced' currently selected.

Creating a Static Route

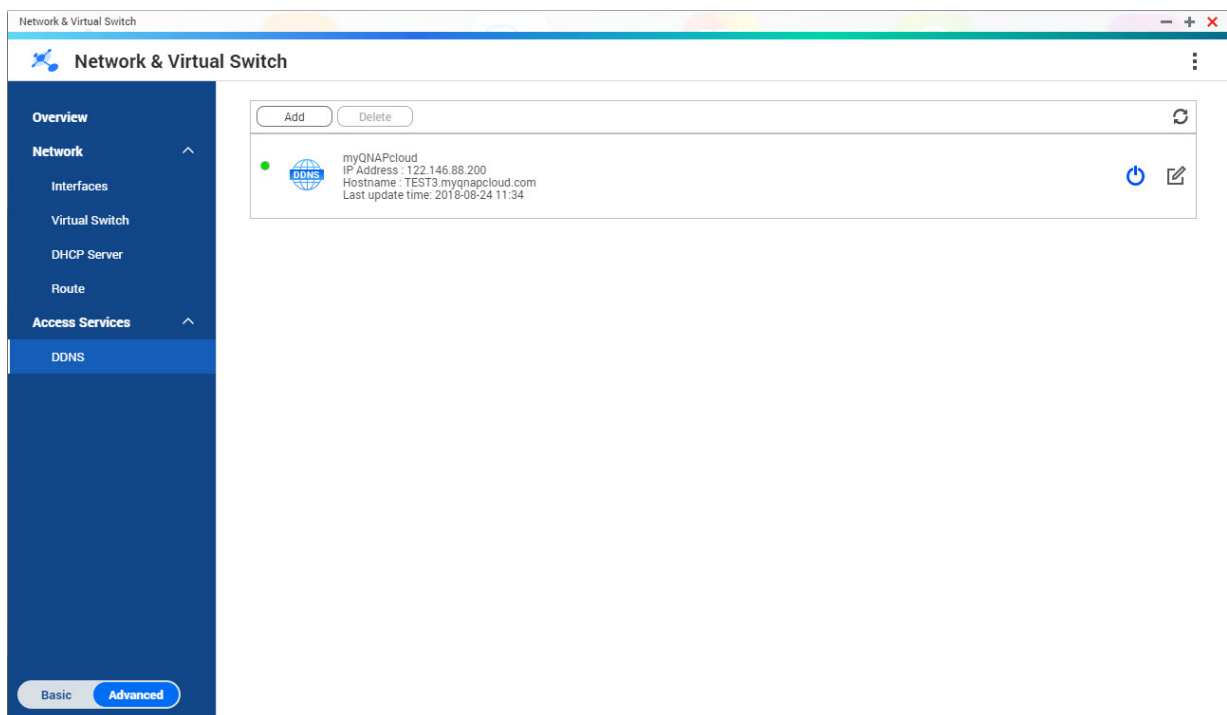
1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Route** .
3. Click **Add**.
The **Static Route (IPv4)** window opens.
4. Configure the IP address settings.

| Setting | Description |
|-------------|---|
| Destination | Specify a static IP address where connections are routed to. |
| Netmask | Specify the IP address of the destination's netmask. |
| Gateway | Specify the IP address of the destination's gateway. |
| Metric | Specify the number of nodes that the route will pass through. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Note Metrics are cost values used by routers to determine the best path to a destination network.</p> </div> </div> |
| Interface | Select the interface that connections should be routed through. |

5. Click **Apply**.

DDNS

This screen controls the management of Dynamic Domain Name System (DDNS) services. DDNS allows access to the NAS from the internet using a domain name rather than an IP address.



Adding a DDNS Service

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DDNS** .
3. Click **Add**.
The **DDNS (Add)** window opens.
4. Configure the DDNS settings.

| Setting | Description |
|-------------------------------|---|
| Select DDNS server | Select the DDNS service provider. |
| Username | Specify the username for the DDNS service. |
| Password | Specify the password for the DDNS service. |
| Hostname | Specify the hostname or domain name for the DDNS service. |
| Check the External IP Address | Specify how often to update the DDNS record. |

5. Click **Apply**.

11. Network & File Services

Network Access

Service Binding

NAS services run on all available network interfaces by default. Service binding enables you to bind services to specific network interfaces to increase security. You can bind services to one or more specific wired or wireless network interfaces.



Important

Configuring service binding does not affect users currently connected to the NAS. When users reconnect they will only be able to access the configured services using the specified network interfaces.

Configuring Service Binding

1. Go to **Control Panel > Network & File Services > Network Access > Service Binding** .
2. Select **Enable Service Binding**.
A list of available services and interfaces is displayed.
3. Bind services to interfaces.



Important

- By default, QTS services are available on all network interfaces.
- Services must be bound to at least one interface.



Tip

Click **Use Default Value** to bind all services.

- a. Identify a service.
 - b. Deselect interfaces not bound to the service.
4. Click **Apply**.

Proxy Server

A proxy server acts as an intermediary between the NAS and the internet. When enabled, QTS will route internet requests through the specified proxy server.

Configuring the Proxy Server Settings

1. Go to **Control Panel > Network & File Services > Network Access > Proxy** .
2. Select **Use a proxy server**.
3. Specify the proxy server URL or IP address.
4. Specify a port number.
5. Optional: Configure proxy authentication.

- a. Select **Authentication**.
- b. Specify a username.
- c. Specify a password.

6. Click **Apply**.

Service Ports

QNAP uses designated ports for communication. These ports are assigned to a specific service and users must manually open the required ports by adding the port number.



Note

The port for the enabled service should remain open while configuring the firewall, or while setting up the router for port forwarding or UPnP.

| Service Name | Default Port Number |
|---|--------------------------|
| Apple Filing Protocol (AFP) | 548 |
| BitTorrent | 6681 - 6999 |
| FTP/FTPES | 20, 21 |
| Passive FTP | 55536 - 56559 |
| LDAP server | 389 |
| MySQL database system | 3306 |
| NAS web | 8080 |
| NAS web (HTTPS) | 443 |
| NetBIOS/ Samba | 137, 138, 139, 445 |
| Network File System (NFS) | 2049, 111, dynamic ports |
| QVPN (OpenVPN) | 1194 |
| QVPN (PPTP server) | 1723 |
| QVPN (L2TP/IPSec server) | 500, 4500, 1701 |
| QVPN (QBelt server) | 443 |
| RADIUS authentication | 1645, 1812 |
| RADIUS accounting | 1646, 1813 |
| rsync | 873 |
| Real-time Remote Replication (RTRR) | 8899 |
| Secure Shell (SSH)/SSH File Transfer Protocol (SFTP) server | 22 |
| Simple Mail Transfer Protocol (SMTP) | 25 |
| Simple Network Management Protocol (SNMP) | 161 |
| Syslog | 514 |
| Telnet | 13131 |
| Trivial File Transfer Protocol (TFTP) | 69 |
| TwonkyMedia server (TMS) | 9000 |

| Service Name | Default Port Number |
|--------------------------------|---------------------|
| Virtualization Station | 8088 |
| Virtualization Station (HTTPS) | 8089 |
| Web server (HTTP, HTTPS) | 80, 8081 |

Win/Mac/NFS

Microsoft Networking

Microsoft Networking refers to Samba, a network protocol that allows data to be accessed over a computer network and provides file and print services to Windows clients.

Configuring Microsoft Networking

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > Microsoft Networking**.
2. Select **Enable file service for Microsoft networking**.
3. Configure Microsoft networking settings.




| Setting | User Action |
|--------------------------------------|---|
| Server description (Optional) | Specify a description that contains a maximum of 256 characters. The description must enable users to easily identify the NAS on a Microsoft network. |
| Workgroup | Specify a workgroup name that contains 1 to 15 characters from any of the following groups: <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: ~ ! @ # \$ ^ & () - _ { } . ' . |






4. Select an authentication method.

| Option | Description |
|-----------------------------------|---|
| Standalone server | QTS uses the local user account information for authentication. |
| AD domain member | QTS uses Microsoft Active Directory (AD) for authentication. |
| LDAP domain authentication | QTS uses an LDAP directory for authentication. |

5. Configure the advanced settings.
 - a. Click **Advanced Options**.
The **Advanced Options** window opens.
 - b. Configure the advanced settings.
 - c. Configure any of the following settings.

| Option | User Action |
|---------------------------|---|
| Enable WINS server | Select this option to run a WINS server on the NAS. |

| Option | User Action |
|--|---|
| Use the specified WINS server | Select this option to specify a WINS server IP address that QTS will use for name resolution. |
| Local master browser | <p>Select this option to use the NAS as a local master browser. A local master browser is responsible for maintaining the list of devices in a specific workgroup on a Microsoft network.</p> <p> Important To use the NAS as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".</p> |
| Allow only NTLMSSP authentication | Select this option to authenticate clients using only NT LAN Manager Security Support Provider. When this option is deselected, QTS uses NT LAN Manager (NTLM). |
| Name resolve priority | Select a name service to use for name resolution. The default service is DNS only . If a WINS server is specified, Try WINS then DNS is selected by default. |
| Alternative login Style | Select this option to change how usernames are structured when accessing FTP, AFP, or File Station services. After selecting this option, users can access NAS services using Domain\Username, instead of Domain+Username. |
| Automatically register in DNS | Select this option to register the NAS on the DNS server. If the NAS IP address changes, the NAS automatically updates the IP address on the DNS server. This option is only available if AD authentication is enabled. |
| Enable trusted domains | Select this option to join users from trusted AD domains. This option is only available if AD authentication is enabled. |
| Enable Asynchronous I/O | <p>Select this option to improve the Samba performance using asynchronous I/O. Asynchronous I/O refers to the I/O behavior on the CIFS protocol layer. This is different from the synchronous I/O feature found in the shared folder settings, which only applies to specific shared folders on the file system level.</p> <p> Tip To prevent power interruption, use a UPS when asynchronous I/O is enabled.</p> |
| Enable WS-Discovery to help SMB clients discover the NAS. | Select this option to enable Web Services Dynamic Discovery (WS-Discovery). WS-Discovery makes the NAS visible in File Explorer on Windows 10 computers. |
| Highest SMB version | <p>Select the highest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.</p> <p> Note Selecting SMB3 will also include SMB3.1 and SMB3.1.1.</p> |

| Option | User Action |
|---|---|
| Lowest SMB version | <p>Select the lowest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.</p> <p> Note Selecting SMB3 will also include SMB3.1 and SMB3.1.1.</p> |
| Allow Symbolic links within a shared folder | <p>Select this option to allow symbolic links within shared folders.</p> <p> Important You must enable this setting in order to restore files from snapshots on Windows using Windows Previous Versions. For details, see Snapshot Data Recovery.</p> |
| Allow Symbolic links between different shared folders | <p>Select this option to allow symbolic links between shared folders.</p> <p> Note This setting requires Allow Symbolic links within a shared folder to be selected first.</p> |
| Restrict anonymous users from accessing SMB shared folders | <p>Select this option to require users to log in before accessing SMB shared folders.</p> <p> Note This setting will be locked to Enabled (strict) if ABSE is enabled on any shared folder.</p> |
| Veto files | <p>This option enables you to hide files from users accessing the NAS via SMB. Files are hidden if their filename matches a pattern in the veto criteria file.</p> |
| Veto criteria | <p>Specify filename criteria for hiding files from SMB NAS users.</p> <p> Note This option is only available when Veto files is selected.</p> |

- d. Click **Apply**.
The **Advanced Options** window closes.

6. Click **Apply**.

Apple Networking

The Apple Filing Protocol (AFP) is a file service protocol that allows data to be accessed from a macOS device.

Configuring Apple Networking

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > Apple Networking**.
2. Select **Enable AFP (Apple Filing Protocol)**.
3. Optional: Select **DHX2 authentication support**.
4. Click **Apply**.

NFS Service

Network File System (NFS) is a file system protocol that allows data to be accessed over a computer network. Enabling the NFS service allows Linux and FreeBSD users to connect to the NAS.

Enabling the NFS Service

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS > NFS Service** .
2. Enable NFS Service.
 - a. Optional: Click **Enable NFS v2/v3 Service**.
 - b. Optional: Click **Enable NFS v4 Service**.
3. Click **Apply**.

Telnet/SSH

Telnet is a network protocol used to provide a command line interface for communicating with the NAS.

Secure Shell (SSH) is a network protocol used for securely accessing network services over an unsecured network. Enabling SSH allows users to connect to the NAS using an SSH-encrypted connection or a SSH client such as PuTTY.

SSH File Transfer Protocol (SFTP) is a secure network protocol that works with SSH connections to transfer files and navigate through the QTS filesystem. SFTP can be enabled after allowing SSH connections on the NAS.

Configuring Telnet Connections



Important

Only administrator accounts can access the NAS through Telnet.

1. Go to **Control Panel > Network & File Services > Telnet/SSH** .
2. Select **Allow Telnet connection**.
3. Specify a port number.
Port numbers range from 1 to 65535.



Tip

The default Telnet port is 13131.

4. Click **Apply**.

Configuring SSH Connections



Important

Only administrator accounts can access the NAS through SSH.

1. Go to **Control Panel > Network & File Services > Telnet/SSH** .
2. Select **Allow SSH connection**.
3. Specify a port number.

Port numbers range from 1 to 65535.



Tip

The default SSH port is 22.

4. Optional: Select **Enable SFTP**.
5. Click **Apply**.

Editing SSH Access Permissions

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.
2. Click **Edit Access Permission**.
The **Edit Access Permission** window opens.
3. Select user accounts to give access permissions.



Important

Only administrator accounts can log in using an SSH connection.

4. Click **Apply**.

SNMP



The Simple Network Management Protocol (SNMP) is used to collect and organize information about managed devices on a network. Enabling the QTS SNMP service allows for the immediate reporting of NAS events, such as warnings or errors, to a Network Management Station (NMS).

Configuring SNMP Settings

1. Go to **Control Panel > Network & File Services > SNMP**.
2. Select **Enable SNMP Service**.
3. Configure the SNMP settings.

| Setting | User Action |
|------------------------|---|
| Port number | Specify the port that the Network Management Station (NMS) will use to connect to QTS. |
| SNMP Trap Level | Select the type of alert messages that the NAS will send to the NMS. <ul style="list-style-type: none"> • Information: QTS sends information regarding ongoing or scheduled NAS operations. • Warning: QTS sends alerts when NAS resources are critically low or the hardware behaves abnormally. • Error: QTS sends alerts failing to enable or update NAS features or applications. |
| Trap Address | Specify the IP addresses of the NMS. You can specify a maximum of 3 trap addresses. |

4. Select the SNMP version that the NMS uses.

| Option | User Action |
|-------------------|--|
| SNMP V1/V2 | <p>Specify an SNMP community name that contains 1 to 64 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 <p>The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and the NAS. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.</p> |
| SNMP V3 | <p>Specify the username, authentication protocol and password, and privacy protocol and password.</p> <p>a. Specify a username.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p> Note The username should contain 1 to 32 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 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ </div> <p>b. Optional: Select Use Authentication.</p> <ol style="list-style-type: none"> 1. Specify the authentication protocol. <div style="border-left: 2px solid #FFC000; padding-left: 10px; margin-left: 20px;"> <p> Tip You can select either HMAC-MD5 or HMAC-SHA. If you are unsure about this setting, QNAP recommends selecting HMAC-SHA.</p> </div> <ol style="list-style-type: none"> 2. Specify an authentication password that contains 8 to 64 ASCII characters. <p>c. Optional: Select Use Privacy.</p> <ol style="list-style-type: none"> 1. Specify a privacy password that contains 8 to 64 ASCII characters. |

5. Click **Apply**.

SNMP Management Information Base (MIB)

The Management Information Base (MIB) is a type of database in ASCII text format that is used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the NAS status or understand the messages that the NAS sends within the network. You can download the MIB and then view the contents using any word processor or text editor.

**Important**

MIBs describe the structure of the management data of a device subsystem. They use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that you can read or set using SNMP. You must assign the correct OID to retrieve the NAS information. The default OID for QNAP NAS devices is 1.3.6.1.4.1.24681.2.

Downloading the SNMP MIB

1. Go to **Control Panel > Network & File Services > SNMP** .
2. Under **SNMP MIB**, click **Download**.
QTS downloads the NAS.mib file on your computer.

Service Discovery**UPnP Discovery Service**

Universal Plug and Play (UPnP) is a networking technology that enables the discovery of networked devices connected to the same network. After enabling this service, devices supporting UPnP can discover the NAS.

Enabling the UPnP Discovery Service

1. Go to **Control Panel > Network & File Services > Service Discovery > UPnP Discovery Service** .
2. Select **Enable UPnP Discovery Service**.
3. Click **Apply**.

Bonjour

Bonjour is a networking technology developed by Apple that enable devices on the same local area network to discover and communicate with each other.

Enabling Bonjour

1. Go to **Control Panel > Network & File Services > Service Discovery > Bonjour** .
2. Select **Enable Bonjour Service**.
3. Select the services to be advertised by Bonjour.

**Important**

You must enable the services in QTS before advertising them with Bonjour.

4. Click **Apply**.


FTP

The NAS FTP service helps optimize FTP data transfer. To use the service, you must configure the settings and then connect the NAS to an FTP client such as FileZilla.

Configuring FTP Settings

1. Go to **Control Panel > Network & File Services > FTP > FTP Service** .
2. Select **Enable FTP Service**.

3. Configure the followings settings.

| Setting | User Action |
|---|---|
| Protocol type | Select at least one FTP type: <ul style="list-style-type: none"> • FTP (standard) • FTP with SSL/TLS (explicit) |
| Port number | Specify a port number between 1 and 65535 |
| Unicode support | Specify whether you want to enable Unicode support for filenames |
| Enable anonymous | Select Yes to allow anonymous users to access files via FTP. |
| Connection | |
| Maximum number of all FTP connections | Specify a value between 2 and 1024 |
| Maximum number of connections for a single account | Specify a value between 2 and 1024 |
| Enable FTP transfer limitation | Enable this option to specify the maximum upload and download rate |
| Maximum upload rate (KB/s) | Select this option to specify the maximum upload rate of files over FTP. You must specify a value of at least 1. |
| Maximum download rate (KB/s) | Select this option to specify the maximum download rate of files over FTP. You must specify a value of at least 1. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note The maximum number of allowed connections for a single account must be lower than the maximum number of total allowed FTP connections.</p> </div> |

4. Click **Apply**.

Configuring Advanced FTP Settings

1. Go to **Control Panel > Network & File Services > FTP > FTP Service** .
2. Select **Enable FTP Service**.
3. Go to **Advanced**.
4. Configure the following advanced FTP settings.

| Setting | Description |
|--|--|
| Passive FTP Port Range | You can use the default port range (55536-56559) or specify a port range larger than 1023. When using this function, make sure you have opened the ports on your router or firewall. |
| Respond with external IP address for passive FTP connection request | Enable this function when a passive FTP connection is in use, the FTP server (NAS) is behind a router, and a remote computer cannot connect to the FTP server over the WAN. When this is enabled, the NAS replies with the specified IP address or automatically detects an external IP address so that the remote computer is able to connect to the FTP server. |

| Setting | Description |
|---------------------------|--|
| Set root directory | After enabling this function and selecting a root directory, only that directory will be visible to FTP users. Otherwise, all of the shared folders will be visible. |



5. Click **Apply**.

Network Recycle Bin

The Network Recycle Bin contains files deleted from the NAS through File Station, QuFTP, or by clients connected using Microsoft networking.

Configuring the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin**.
2. Select **Enable Network Recycle Bin**.
3. Optional: Configure the Network Recycle Bin settings.

| Setting | Description |
|--------------------------------------|--|
| File retention time | Specify the number of days files are retained. The Daily check time controls when recycled files are checked against the retention time.  Tip This field supports a maximum of 9999 days. The default is 180 days. |
| Exclude these file extensions | Specify which file extensions are excluded from the Network Recycle Bin.  Important File types are case insensitive and must be separated by a comma. |


4. Click **Apply**.

Deleting All Files in the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin**.
2. Click **Empty All Network Recycle Bin**.
A warning message appears.
3. Click **OK**.
QTS deletes all files from the Network Recycle Bin.

Restricting Access to the Network Recycle Bin

1. Go to **Control Panel > Privilege > Shared Folders**.
2. Identify a shared folder.

3. Under **Actions**, click .
The **Edit Properties** window appears.
4. Select **Enable Network Recycle Bin**.
5. Select **Restrict the access to Recycle Bin to administrators only for now**.
6. Click **OK**.

12. myQNAPcloud

myQNAPcloud is a service that allows you to access, manage, and share files stored on your QNAP devices remotely through the internet.

Getting Started

1. Create a QNAP ID.
For details, see [Creating a QNAP ID With Email or Phone Number](#).
2. Register the device to myQNAPcloud.
For details, see [Registering a Device to myQNAPcloud](#).
3. Optional: Configure any of the following settings.

| Settings | Description |
|--------------------|--|
| Port forwarding | Port forwarding allows you to access your device on the internet through a UPnP router. For details, see Configuring Port Forwarding . |
| My DDNS | My DDNS allows you to specify a dedicated myQNAPcloud subdomain name that you can use to access your device on the internet. For details, see Configuring DDNS Settings . |
| Published services | You can publish QNAP services on your device, such as the QNAP desktop and File Station, so they can be accessible on myQNAPcloud. For details, Configuring Published Services . |
| myQNAPcloud Link | myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to client device. For details, see Enabling myQNAPcloud Link . |
| Access controls | Access controls allow you to configure device access permissions for myQNAPcloud users. For details, see Configuring Device Access Controls . |
| SSL certificates | myQNAPcloud allows you to add SSL certificates to help secure your network communication. You can either download and install a myQNAPcloud or Let's Encrypt certificate. For details, see Installing an SSL Certificate . |

Account Setup

Before using myQNAPcloud services, you must first create a QNAP ID and then configure required settings using your QNAP ID.

Creating a QNAP ID With Email or Phone Number

1. Go to <https://account.qnap.com/>.
The **QNAP Account** login page displays.
2. Click **Create Account**.
The **Create Account** screen appears.
3. Specify a nickname, a valid email address or phone number, and a password.
4. Read and acknowledge the Terms of Service and Privacy Policy.

5. Click **Sign Up**.
The **Data Privacy Notice** box appears.
6. Read the notice, and then click **I Agree**.
myQNAPcloud sends a verification email or message.
7. Confirm the registration.
Your QNAP ID is activated.

**Tip**

The registration link automatically expires in 15 days. You can go to [QNAP Account](#) to send a new activation email.

Registering a Device to myQNAPcloud

1. Log on to QTS as administrator.
2. Go to **myQNAPcloud > Overview** .
3. Click **Get Started**.
The **myQNAPcloud wizard** appears.
4. Click **Start**.
5. Specify your QNAP ID and password.
6. Click **Next**.
7. Specify a device name containing up to 30 alphanumeric characters.
You may reuse an existing device name. The device currently using this name will be deregistered from myQNAPcloud.
8. Click **Next**.
9. Select the services you want to enable.

| Service | Description |
|----------------------------------|--|
| Auto Router Configuration | This allows you to configure port forwarding. |
| DDNS | This allows you to access your device on the internet using a dedicated address. |
| Published Services | This allows you to select which services you want to publish on the myQNAPcloud website. |
| myQNAPcloud Link | myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to client device. If you enable this option and your device does not have myQNAPcloud Link, myQNAPcloud Link will automatically be downloaded and installed after you click Next . |

10. Select an access control option.


| Option | Description |
|---------------|--|
| Public | All users can search for your device and view the published services on the myQNAPcloud website. They can also access your device with a SmartURL. |

| Option | Description |
|-------------------|---|
| Private | Your device will not appear in the search results. Only you can access your device on the myQNAPcloud website. |
| Customized | Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL. |

- Click **Next**.
myQNAPcloud applies your settings.
The **Summary** screen appears.
- Review the details, and then click **Finish**.





Installing myQNAPcloud Link






Only perform this task if you did not enable myQNAPcloud Link when registering your device to your myQNAPcloud account.


- Log on to QNAP as administrator.
- Open **App Center**.
- Click .
A search box appears.
- Type `myQNAPcloud Link` and then press `ENTER`.
The myQNAPcloud Link application appears in the search results list.
- Click **Install**.
App Center installs myQNAPcloud Link on your device.

Overview

The **Overview** screen displays your basic myQNAPcloud settings, as well as the device network connectivity and DDNS status.

| Status Icon | Description |
|---|---|
|  | The item is enabled and functioning properly. |
|  | The item is disabled. |
|  | One or more settings need to be configured for the item to function properly. |
|  | There is no network connectivity. |

| Button | Description |
|---|--|
|  | Click this to view your QNAP ID details. |
|  | Click this to sign out of myQNAPcloud. |
|  | Click this to modify your device name. |
|  | Click this to copy the SmartURL to your clipboard. |
|  | Click this to open the myQNAPcloud FAQ page on your browser. |

| Button | Description |
|---|---|
|  | Click this to diagnose connection problems. |
| Test | Click this to test the internet connectivity. |

Configuring Port Forwarding

Port forwarding is only available if your router supports UPnP.

1. Go to **Auto Router Configuration**.
2. Select **Enable UPnP port forwarding**.
Your device scans for UPnP routers on the network.



Tip

If your device cannot locate the router, click **Rescan**. If the issue persists, click **Diagnostics**, and then verify your network configuration or contact QNAP support through **Helpdesk**.

3. Optional: Add a new service to the **Forwarded Services** table.
 - a. Click **Add NAS Service**.
The **Add NAS Service** window appears.
 - b. Specify a NAS service name that contains 1 to 64 ASCII characters.
 - c. Specify a port number.
 - d. Select an external port setting.
 - **Auto**: myQNAPcloud automatically selects an available external port.
 - **Manual**: You can specify a new port if the current service port is being used by other services.
 - e. Select a protocol.
If you are unsure about this setting, select **TCP**.
 - f. Click **OK**.
4. In the **Forwarded Services** table, select the services you want to forward.
5. Click **Apply to Router**.



Tip

You can go to **Overview** to verify that there are no connectivity errors.

Configuring DDNS Settings

1. Open myQNAPcloud.
2. Go to **My DDNS**.
3. Enable **My DDNS**.
4. Perform any of the following tasks.

| Task | User Action |
|---|--|
| Change the myQNAPcloud DDNS domain name | <ol style="list-style-type: none"> a. Click here. The Change Device Name Wizard appears. b. Specify a device name containing up to 30 alphanumeric characters. c. Click Apply. |
| Update myQNAPcloud | Click Update . |
| Manually configure the DDNS IP address | <ol style="list-style-type: none"> a. Click Manually configure your DDNS IP address. The Public IP Address window appears. b. Select an option. <ul style="list-style-type: none"> • Assign static IP addresses: myQNAPcloud binds the DDNS to the specified static IP address regardless of changes to the network environment. • Automatically obtain IP address: myQNAPcloud automatically detects the WAN IP. c. Click Apply. |

Restarting DDNS Service

DDNS service may sometimes be disabled or suspended due to security concerns. You can restart the DDNS service in myQNAPcloud to regain access to the service.

1. Clear the cache on your web browser.
2. Log on to QTS as administrator.
3. Open myQNAPcloud.
4. Go to **My DDNS**.
5. Disable **My DDNS**.
6. Enable **My DDNS**.

myQNAPcloud DDNS service is restarted and resumed.



Tip

If you still cannot connect to the NAS via myQNAPcloud DDNS, the service may be temporarily blocked by your Internet Service Provider (ISP). Wait at least two hours before attempting to restart the DDNS service.

Configuring Published Services

1. Open myQNAPcloud.
2. Go to **Published Services**.
3. In the **Publish** column, select all the services you want published.
Published services are accessible through the myQNAPcloud website.
4. Optional: In the **Private** column, select all the services you want publish privately.
Private services are only available to specified users with the access code.

- a. Specify an access code containing 6 to 16 alphanumeric characters.
- b. In the **User Management** table, select the users you want to grant access to.
You can select a maximum of 9 users.

**Tip**

Click **Add Users** to add users to the list.
Click **Delete** to remove users from the list.

- c. Optional: Modify user access privileges.

| Option | Description |
|----------------------------------|--|
| myQNAPcloud Connect (VPN) | Select this option to grant users access to private NAS services when they use the myQNAPcloud Connect utility. Users can download myQNAPcloud Connect from the QNAP Utilities page (https://www.qnap.com/en/utilities/essentials). |
| myQNAPcloud Website | Select this option to grant users access to private NAS services published in the myQNAPcloud website (https://www.myqnapcloud.com/). |

5. Click **Apply**.

Enabling myQNAPcloud Link

1. Open myQNAPcloud.
2. Go to **myQNAPcloud Link**.
3. Enable **myQNAPcloud Link**.


**Tip**

If there are issues with the connection, click **Reconnect**.

Configuring Device Access Controls

1. Open myQNAPcloud.
2. Go to **Access Control**.
3. Select an access control option.

| Option | Description | User Action |
|---------|--|-------------------------|
| Public | All users can search for your device and view the published services on the myQNAPcloud website. | Select Public . |
| Private | Your device will not appear in the search results. Only you can access your device on the myQNAPcloud website. | Select Private . |

| Option | Description | User Action |
|------------|--|--|
| Customized | Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL | <p>a. Select Customized.</p> <p>b. Optional: Add a user.</p> <ol style="list-style-type: none"> 1. Click Add. 2. Specify the user's email address or phone number. 3. Click . <p>c. Optional: Remove a user.</p> <ul style="list-style-type: none"> • From the list of users, identify a user you want to remove. • Click ×. |

4. Click **Apply**.

Installing an SSL Certificate



Important

myQNAPcloud SSL web service and Let's Encrypt certificates can only be used with the myqnnapcloud domain.

1. Open myQNAPcloud.
2. Go to **SSL Certificate**.
3. Download and install a certificate.

| Type | Description | User Action |
|---|--|---|
| myQNAPcloud SSL web service certificate | This certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users. You can purchase certificates on the myQNAPcloud website. | <p>a. Under myQNAPcloud SSL Certificate, click Download and install. The Download & Install SSL Certificate window appears.</p> <p>b. Select a license from the list. A notification appears if you have not yet purchased a myQNAPcloud certificate.</p> |
| Let's Encrypt certificate | Let's Encrypt is a free, automated, and open certificate authority that issues domain-validated security certificates. You can install Let's Encrypt certificates with the myQNAPcloud DDNS service. You can choose to automatically renew this certificate before it expires. | <p>a. Under Let's Encrypt, click Download and install. The Download & Install SSL Certificate window appears.</p> <p>b. Specify a valid email address. This address is required for the Let's Encrypt account registration.</p> <p>c. Optional: Select Automatically renew domain before expiration.</p> |

4. Click **Confirm**.
myQNAPcloud applies the certificate and displays the details.

**Tip**

To delete the certificate from the device, click **Release** and then **Confirm**.

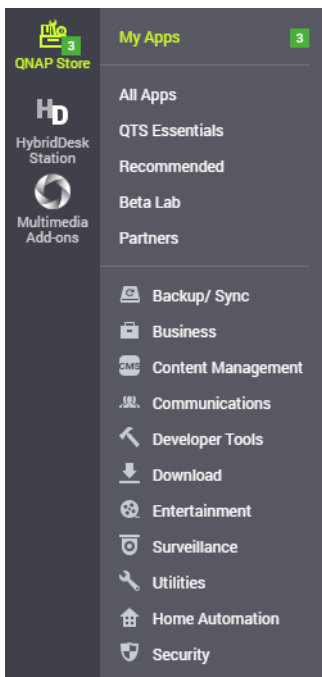
13. App Center

App Center is a digital distribution and management platform in QTS where you can browse, download, and manage applications and utilities developed for the QNAP NAS.

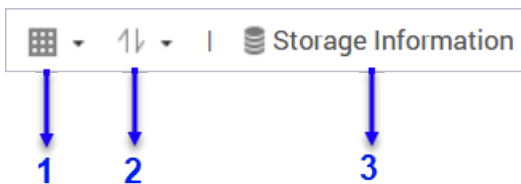
Overview

Left Panel

The left panel allows you to browse available apps in various categories. You can go to the **My Apps** section to view all your installed apps. App Center displays a badge count to indicate the number of available updates.



Toolbar



Left side

| No. | Elements | Possible User Actions |
|-----|-------------|---|
| 1 | View mode | <ul style="list-style-type: none"> Click the icon to switch between two view modes. Click \wedge and select a view mode. |
| 2 | App sorting | Click \wedge and select an app sorting method. |

| No. | Elements | Possible User Actions |
|-----|--------------------|---|
| 3 | Volume information | View the basic volume information and the installation locations of your apps. For more volume information, click Details . |

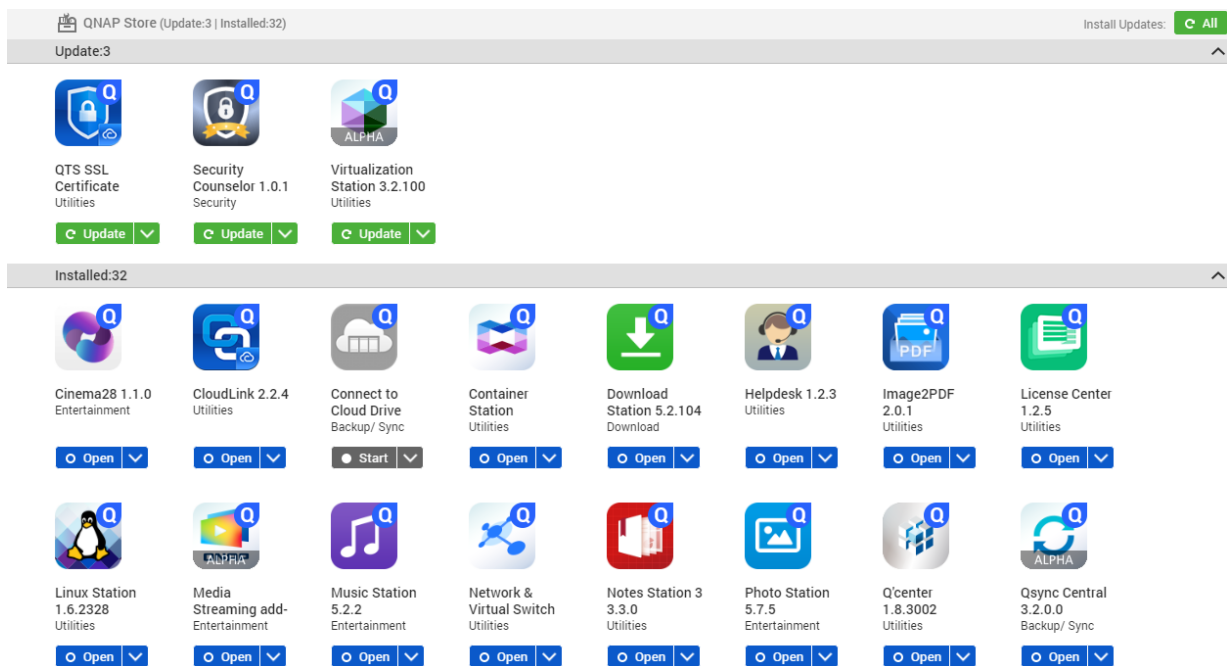


Right side

| No. | Elements | Possible User Actions |
|-----|---------------------|--|
| 1 | Search | Specify keywords to search for apps. App Center instantly displays search results based on specified keywords. |
| 2 | Refresh | Reload the data in App Center to view the current status of your apps. |
| 3 | Manual installation | Manually install an app by uploading an installation package. For details, see Installing an App Manually . |
| 4 | Settings | Configure various App Center settings. For details, see App Center Settings . |
| 5 | More | View the Quick Start or the Help document for more information about App Center. |

Main Area

The main area allows you to browse available apps and manage your installed apps. For details, see [App Management](#).



App Management

The App Center allows you to enable or disable an app, assign CPU resources to load-intensive apps, update apps, and configure app update settings.

Viewing App Information

You can browse apps and view their descriptions in App Center. This helps you decide whether to install or update an app.

1. Open App Center.
2. Locate an app.
3. Click the app icon.
App Center displays the app information in a new window.
4. Perform one of the following actions.
 - View the app description
 - View the app changelog
 - Go to the QNAP forum
 - Download the app installation package

Subscribing to an App License

1. Open App Center.
2. Go to the app.
3. Click **Subscribe License**.

- The **Software Store** window opens in a separate browser tab.



Important

For details about license subscription or purchasing a license from [Software Store](#), see [Licenses](#).

- The **License Center** window appears.



Important

For details about activating the license subscription, see [Licenses](#).

Installing an App from App Center



Warning

QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.



Important

- Certain apps require activating a subscription or license before app installation. For details, see [Licenses](#).
- Based on the app you choose to install, App Center may display a confirmation message that provides more information and asks for your approval for installation. Certain apps also require you to specify the installation location. Read the message carefully before installing the app.

1. Open App Center.
2. Locate an app.
3. Optional: Click the app icon to view the app information.
4. Click **Install**.
The app is installed.

Installing an App Manually



Warning


- QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.
- App Center does not allow the installation of invalid apps, including apps with invalid digital signatures, apps not approved by App Center, or from [Software Store](#). If App Center detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.



Important

Certain apps require activating a subscription or license before app installation. You can go to [Software Store](#) to purchase an app license or subscription. For details about activating an app license, see [Licenses](#).

1. Open App Center.

2. Click  on the toolbar.
The **Install Manually** window appears.
3. Click **Browse**.
4. Locate and select the installation package.
5. Click **Install**.
A message appears.
6. Depending on the scenario, perform one of the following actions.

| Scenario | Actions |
|--|---|
| The app has a valid digital signature. | <ol style="list-style-type: none"> a. Read the confirmation message. b. Click OK. |
| The app does not have a valid digital signature, and you enabled the installation of apps without valid digital signatures. | <ol style="list-style-type: none"> a. Read the confirmation message. b. Click OK. |
| The app does not have a valid digital signature, and you did not enable the installation of apps without valid digital signatures. | <ol style="list-style-type: none"> a. Read the warning message. b. Select I understand the risks and want to install this application. c. Click Install. |



Tip

For more information on this setting, see [Enabling Installation of Apps without Digital Signatures](#).

App Center installs the app.

Updating an App

When updates are available for an installed app, App Center moves the app to the **Update** or **Required Update** section based on the importance of updates. You must perform required updates to ensure the functionality, compatibility, and data security of your apps.

1. Open App Center.
2. Locate an app in the **Update** or **Required Update** section.
3. Click **Update** or **Required Update**.
A confirmation message appears.
4. Click **OK**.

Batch Updating Multiple Apps

1. Open App Center.
2. Perform one the following updates.

| Updates | Action |
|-----------------------|---|
| Only required updates | Below the toolbar, click Required Update . |

| Updates | Action |
|-----------------------|---------------------------------------|
| All available updates | Below the toolbar, click All . |

A confirmation message appears.

3. Click **OK**.

Enabling or Disabling an App


You can enable or disable non-built-in apps in App Center.



Note

- Disabling an app may affect the functionality of other apps.
- Disabling an app does not remove or uninstall the app.


1. Open App Center.
2. Locate an app.
3. Perform one of the following actions.

| Action | Steps |
|-----------------|---|
| Enable the app | Click Start . |
| Disable the app | <ol style="list-style-type: none"> a. Click . b. Select Stop. |

- After an app is enabled, its action button displays **Open**.
- After an app is disabled, its action button displays **Start**.


Migrating an App

You can migrate an installed app to another volume to better allocate system resources.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Migrate to**.
The **App Migration** window appears.
5. Select the destination volume.
6. Click **Migrate**.
A confirmation message appears.
7. Click **OK**.

Granting or Denying User Access to an App

QTS administrators can grant or deny user access to apps. The main menu of non-administrator users only display the apps that they have access to.

1. Open App Center.
2. Locate an app.
3. Click .
4. Hover the mouse pointer over **Display on**.
5. Select one of the following options:
 - Administrator's main menu



Note

This is the only available option for many built-in system utilities, which non-administrators cannot be granted access to.


- Every user's main menu
- Every user's main menu and as an app shortcut on the login screen

Uninstalling an App



Warning


Uninstalling an app also deletes the related user data.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Remove**.
A confirmation message appears.
5. Click **OK**.

App Center Settings

Adding an App Repository

You can add an app repository to enrich the content in App Center. This allows you to download and install apps from third-party sources.

1. Open App Center.
2. Click  on the toolbar.
3. Go to **App Repository**.
4. Click **Add**.
The **Add** window appears.

5. Specify the following connection information.

- Name
- URL

6. Optional: Specify the login credentials.


- Username
- Password

7. Click **Add**.

App Center adds the repository to the list. You can select the repository and then click **Edit** to modify its settings or click **Delete** to remove this repository from App Center.

Configuring App Update Settings

1. Open App Center.
2. Click  .
3. Go to **Update**.
4. Select **When updates are available** and then select one of the following options.

| Option | Description |
|---|--|
| Send a notification | <p>QTS sends notification messages when updates are available for your apps. You can click Configure Notification Rule to create rules in Notification Center. For details, see Notification Center.</p> <p> Note If you select this option, the system will skip the check for updates frequency step.</p> |
| Install all updates automatically | <p>App Center automatically installs all available updates for your apps. You can select how often App Center should check for available updates.</p> |
| Install all required updates automatically | <p>App Center automatically installs all required updates for your apps to ensure their functionality, compatibility, and data security. You can select how often App Center should check for required updates.</p> |

5. Select a check for updates frequency.

6. Click **Apply**.

Digital Signatures

QNAP uses digital signatures to validate apps created by QNAP or QNAP-trusted publishers. The use of digital signatures prevent the unauthorized tampering of apps that may lead to security risks.

A digital signature is considered valid if it meets the following criteria.

- The digital signature has not been tampered with.


- The digital signature has not expired.
- The digital signature is certified by QNAP.

Enabling Installation of Apps without Digital Signatures



Warning

- A valid digital signature ensures that an application was created by QNAP or a QNAP-trusted publisher. It also ensures that the app has not been maliciously tampered with. Installing apps without valid digital signatures may expose your NAS to security risks. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of such apps.
- App Center does not allow the installation of invalid apps, including apps with invalid digital signatures, apps unapproved by App Center, or from [Software Store](#). If App Center detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.

1. Open App Center.
2. Click  on the toolbar.
The **Settings** window appears.
3. Go to **General**.
4. Select **Allow installation and execution of applications without a digital signature**.



Important

App Center does not allow the installation of apps with tampered digital signatures even when this setting is enabled.

5. Click **Apply**.

14. Licenses

QNAP licenses enable users to gain access to certain advanced features or premium products. This chapter introduces important concepts and demonstrate essential tasks to help you start using QNAP licenses.

About QNAP Licenses

QNAP offers a wide variety of licenses. Some basic licenses are provided free of charge. You can purchase premium licenses to further enhance the functionality of your QNAP products. QNAP also provides multiple management portals, flexible subscription plans, and various activation options to meet your different needs.

License Types and Plans

The licensing mechanisms and available plans of QNAP licenses vary depending on corresponding software products. They can be divided into the following categories.

License Types

| License Types | Description |
|---------------|--|
| Device-based | <ul style="list-style-type: none"> Allows users to use a software product installed on hardware devices, such as applications. Multi-seat licenses can be activated and used on multiple devices. |
| Floating | <ul style="list-style-type: none"> Allows users to use a software product in the cloud or on a virtual platform, such as QuTScLOUD and applications in QuTScLOUD. Can be activated and used on a limited number of devices at a time |
| User-based | <ul style="list-style-type: none"> Allows a limited number of authorized users to access a web-based service, such as Qmiix. |

License Plans

| License Plans | Description |
|---------------|---|
| Subscription | Authorizes users to use a software product with a recurring monthly or annual fee |
| Perpetual | Authorizes users to use a software product indefinitely |
| One-time | Authorizes users to use a software product within a predefined period of time |

Validity Period

The validity period of a QNAP subscription-based license starts from the date of purchase, not from the date of activation.

For example, if a user starts the subscription of an annual license on January 1, 2020, the next billing date will be January 1, 2021, regardless of the date of activation. If the user cancels the subscription, the license will still remain valid until January 1, 2021.

If the user unsubscribes from a license but subscribes to the same product later, the validity period and billing cycle will begin from the date of the new subscription.

License Portals and Utility

| Portal | Description | URL |
|------------------------|--|---|
| QNAP Software Store | The QNAP Software Store is a one-stop shop where you can purchase licenses for QNAP and QNAP-affiliated software. | https://software.qnap.com |
| QNAP License Center | The QNAP License Center allows you to monitor and manage licenses of applications running on your local device. | - |
| QNAP License Manager | QNAP License Manager is a portal that allows you and your organizations to remotely activate and manage licenses under your QNAP ID. | https://license.qnap.com |
| Old QNAP License Store | Users of QTS 4.3.4 (or earlier) can purchase licenses from this online store. | https://license2.qnap.com |

Software Store

Software Store allows you to purchase licenses for applications. Through Software Store, you can perform the following actions.

- Purchase or upgrade licenses
- Manage your account information
- View purchased subscriptions
- Cancel your subscriptions
- Request a refund for your orders

License Center

License Center allows you to monitor and manage the licenses of your applications running on your local device. Through License Center, you can perform the following actions.

- Activate and deactivate licenses either online or offline
- Remove licenses from the local device
- Recover licenses if your device is reset, reinitialized, or restored to factory default
- Transfer licenses purchased from the old QNAP License Store to the new QNAP License Manager

License Manager

License Manager is a portal that allows you to manage all licenses under QNAP IDs and organizations. Through License Manager, you can perform the following actions.

- View details of your licenses
- Activate and deactivate licenses
- Assign a user-based license to a QNAP ID

**Important**

To remotely activate or deactivate licenses, you must enable myQNAPcloud Link on your QNAP device.

Buying a License Using QNAP ID

Before buying a license, ensure the following.

- The application is already installed on your device.
 - You are signed in to myQNAPcloud.
1. Go to <https://software.qnap.com/>.
 2. Sign in with your QNAP ID.
 3. Locate the product on the list, and then click **Buy** or **Subscribe Now**. The license details appear.
 4. Select the item you want to buy, and then review the price.
 5. Click **Checkout Now**.

**Tip**

You can also click **Add to Cart** and then continue shopping.

The purchase summary page appears in your web browser.

6. Select a payment method.

| Payment Method | User Action |
|----------------|--|
| Credit card | <ol style="list-style-type: none"> a. Specify your card information. b. Verify the items and the price on the order. c. Agree to QNAP terms and conditions. d. Click Place Order. |
| PayPal | <ol style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Pay with PayPal PayPal authentication window appears. d. Specify your PayPal login credentials. e. Click Next. f. Follow PayPal instructions to complete the payment. |
| Google Pay | <ol style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Buy with Google Pay. Google Pay authentication window appears. d. Follow Google Pay instructions to complete the payment. |

After the payment, you can view order details in **My Orders** and manage your subscriptions in **My Subscriptions**.

You can activate your license right after the purchase or at a later time.

For details, see [License Activation](#).

License Activation

You need to activate purchased licenses to access features provided by the license. You can activate QNAP or QNAP-affiliated licenses using the following methods.

| Activation Method | Description |
|---|--|
| Using QNAP ID | Licenses purchased through Software Store are stored in your QNAP ID account. They can be accessed through both License Center and the QNAP License Manager website. |
| Using a license key | You can generate the 25-character license key after purchasing licenses through the QNAP Software Store . For details, see Generating a License Key . You can use license keys to activate licenses in License Center. For details, see Activating a License Using a License Key . |
| Using a product key | The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. You can use product keys to activate licenses in License Center. For details, see Activating a License Using a Product Key or PAK . |
| Using a product authorization key (PAK) | The 24-character PAK is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you are using NAS devices running QTS version 4.3.4 or older, use PAKs to activate licenses through License Center. If you are using NAS devices running QTS version 4.3.4 or later, you can transfer PAKs purchased from the Old QNAP License Store to NAS devices. For details, see Activating a License Using a Product Key or PAK . |
| Offline | Use this method when the NAS is not connected to the internet. For details, see Activating a License Offline . |



Activating a License Using QNAP ID


Before activating your license, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can activate their licenses using QNAP ID in either Qfinder Pro, License Center, or License Manager.

- Activate your license using one of the following methods.

| Method | Steps |
|----------------|---|
| Qfinder Pro | <p>Qfinder Pro allows you to discover QNAP devices on your local network.</p> <ol style="list-style-type: none"> a. Open Qfinder Pro on your computer. <p> Tip You can download Qfinder Pro from the QNAP website.</p> <ol style="list-style-type: none"> b. Select your device form the list. c. Right-click the device and select License Activation. d. Specify your device username and password. The License Activation windows appears. e. Select Activate with QNAP ID. f. Click Select License. g. Specify your QNAP ID and password. h. Click Select License. i. Select a license from the list. j. Click Activate. License Server activates the license. A confirmation message appears. k. Click Close. The license is activated for the device. |
| License Center | <ol style="list-style-type: none"> a. Open License Center. b. Go to My Licenses. c. Click Activate License. The License Activation window appears. d. Select Activate with QNAP ID. e. Click Select License. f. Select a license from the list. <p> Tip If you select a multi-seat license, you can specify the number of seats that you want to activate.</p> <ol style="list-style-type: none"> g. Click Add. License Center activates the license. A confirmation message appears. h. Click Close. The license appears on the list of active licenses. |

| Method | Steps |
|-----------------|---|
| License Manager | <ul style="list-style-type: none"> a. Open your web browser. b. Go to https://license.qnap.com. c. Sign in with your QNAP ID. d. Locate a license from the license list. e. Click  . The Activate License window appears. f. Select Online Activation. g. Select a device. h. Specify your credentials on the device. i. Click Allow. A confirmation message appears. j. Click OK. License Manager activates the license. k. Click Close. The license appears on the list of active licenses. |

Activating a License Using a License Key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID.

You can activate a license using a license key. After purchasing a license from QNAP Software Store, you can generate a license key from the License Manager website and apply the key in License Center. A license key contains 25 characters and always starts with the letter L.

For details, see [Generating a License Key](#).


1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
The **License Activation** window appears.
4. Select **Activate with a License Key**.
5. Specify the key.
6. Read and agree to the terms of service.
7. Click **Verify Key**.
8. Verify the license information.
9. Optional: Specify the number of seats to activate.

**Note**

This option is only available for licenses that support multiple seats.

10. Click **Activate**.
The license is activated.
A confirmation message appears.
11. Click **Close**.
The license appears on the list of active licenses.


Generating a License Key

1. Open your web browser.
2. Go to <https://license.qnap.com>.
3. Sign in with your QNAP ID.
4. From the list of licenses, select the license you want to generate a key for.
5. Click .
The **Activate License** window appears.
6. Select **License Key**.
License Manager generates the license key.

**Tip**

Click **Renew License Key** to generate a new key.

This renews your license key and protects you from any unauthorized access to your existing license key.

7. Hover the mouse pointer over the license key and click .
Your system copies the license.
8. Click **Done**.

The copied license key can be pasted later for license activation.

Activating a License Using a Product Key or PAK

Before activating a license using a product key or a product authorization key (PAK), ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

You can activate a license with a product key or PAK. You may find a product key printed on a physical copy of your product. A product key contains 25 characters and always starts with the letter P.

On the other hand, you may obtain a product authorization key (PAK) if you purchase a license from the old QNAP License Store. A PAK contains 24 digits of random numbers.


1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.


4. The **License Activation** window appears.
5. Select **Activate with a Product Key or PAK**.
6. Specify the key.
7. Read and agree to the terms of service.
8. Click **Verify Key**.
9. Verify the license information.
10. Click **Activate**.
The license is activated.
A confirmation message appears.
11. Click **Close**.
The license appears on the list of active licenses.

Activating a License Offline

You can activate your license offline if your QNAP device is not connected to the Internet. You first need to generate a device identity file (DIF) from Qfinder Pro or from License Center on your device and then upload the DIF to License Manager in exchange for the license install file (LIF). You can then activate the license using the LIF in Qfinder Pro or in License Center on your device.

1. Choose one of the following methods.

| Methods | User Action |
|---|--|
| Offline activation using Qfinder Pro | <p>Qfinder Pro allows you to discover QNAP devices on your local network.</p> <ol style="list-style-type: none"> a. Open Qfinder Pro on your computer. <div style="display: flex; align-items: center;">  <div> <p>Tip You can download Qfinder Pro from the QNAP website.</p> </div> </div> <ol style="list-style-type: none"> b. Select your device from the list. c. Right-click the device and then select License Activation. d. Specify your username and password. The License Activation window appears. e. Select Offline Activation. |
| Offline activation using License Center | <ol style="list-style-type: none"> a. Log in to your QNAP device. b. Open License Center. c. Go to My Licenses. d. Click Activate License. The License Activation window appears. e. Select Offline Activation. |

2. Read and agree to the Terms of Service.
3. Click **Generate Device Identity File**.
Qfinder Pro or License Center downloads the device identity file (DIF) to your computer.
4. Read the instructions and click **Go to License Manager**.
Your web browser opens the **QNAP License Manager** website.
5. Sign in with your QNAP ID.
6. From the list of licenses, select the license you want to activate.
7. Click  (**Upload Device Identity File**).
The **Activate License** window appears.
8. Click **Browse**.
The file browser appears.
9. Locate and select the DIF from your computer.
10. Click **Upload**.
A confirmation message appears.
11. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
12. Click **Done**.
13. Go back to Qfinder Pro or License Center.
14. In the **License Activation** window, click **Upload License File**.
15. Click **Browse**.
The file browser appears.
16. Locate and select the LIF from your computer.
17. Click **Import**.
Qfinder Pro or License Center uploads the LIF and displays the license summary.
18. Click **Activate**.
The license appears on the list of active licenses.

License Deactivation

You can deactivate QNAP or QNAP-affiliated licenses using the following methods.

| Activation Method | Description |
|-------------------|--|
| Using QNAP ID | Licenses purchased through Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website To deactivate this type of license, see Deactivating a License Using QNAP ID . |
| Offline | Use this method when the NAS is not connected to the internet. For details, see Deactivating a License Offline . |



Deactivating a License Using QNAP ID

Before deactivating your license, ensure the following.


- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can deactivate their licenses using QNAP ID in either License Center or License Manager.


- Deactivate your license using one of the following methods.

| Method | Steps |
|-----------------|--|
| License Center | <ol style="list-style-type: none"> a. Open License Center. b. Go to My Licenses. c. Identify the license you want to deactivate, and then click . The License Deactivation window appears. d. Select Use QNAP ID. e. Read and acknowledge the warning. f. Click Deactivate. A confirmation message appears. g. Click Close. License Center deactivates the license and removes the license from the list of active licenses. |
| License Manager | <ol style="list-style-type: none"> a. Open your web browser. b. Go to https://license.qnap.com. c. Sign in with your QNAP ID. d. From the list of licenses, select the license you want to deactivate. e. Click . The Deactivate License window appears. f. Read and acknowledge the warning. g. Click Deactivate. License Center deactivates the license. A confirmation message appears. h. Click Close. License Center removes the license from the list of active licenses. |

Deactivating a License Offline

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to deactivate, and then click .

The **License Deactivation** window appears.

4. Select **Offline Deactivation**.
5. Read and acknowledge the warning.
6. Read the instructions, and then click **Generate License Uninstall File**.
License Center downloads the license uninstall file (LUF) to your computer.
7. Open your web browser.
8. Go to <https://license.qnap.com>.
9. Sign in with your QNAP ID.
10. From the list of licenses, select the license you want to deactivate.
11. Under **Advanced Options**, click .
The **Deactivate License** window appears.
12. Read and agree to the terms.
13. Click **Offline Deactivation**.
14. Click **Browse**.
The file browser appears.
15. Locate and select the LUF from your computer.
16. Click **Upload**.
QNAP License Manager deactivates the license.
A confirmation message appears.
17. Click **Done**.

License Extension

License Center will notify you soon before any of your subscription-based licenses expire. The exact dates vary depending on the type of your licenses (ranging from one week to one month before the expiration date). You can extend your QNAP or QNAP-affiliated licenses using the following methods.

| Activation Method | Description |
|---------------------------------|--|
| Using QNAP ID | Licenses purchased through License Center or Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website. If you have an existing valid, unused subscription-based license in License Center, you can use this to extend your expiring license. For details, see Extending a License Using QNAP ID . |
| Offline using an unused license | If you have a valid, unused subscription-based license and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using an Unused License . |

| Activation Method | Description |
|-----------------------------|---|
| Offline using a product key | <p>The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package.</p> <p>If you have a valid, unused product key for a subscription-based license, and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using a Product Key.</p> |

Extending a License Using QNAP ID


Before extending licenses, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.
- You have an existing valid, unused license.



Note

Subscription-based licenses will be automatically renewed in License Manager. You cannot manually extend a subscription-based license.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Select an unused license.




Warning

License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

5. Click **Extend**.
License Center extends the license.
A confirmation message appears.
6. Click **Close**.

Extending a License Offline Using an Unused License

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is about to expire, its status is `Expires soon`.

The **License Extension** window appears.

4. Select **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
8. Read and agree to the terms of service.
9. Click **Next**.
10. Read the instructions, and then click **Go to License Manager**.
Your web browser opens the QNAP License Manager website.
11. Sign in with your QNAP ID.
12. Go to **My Licenses**.
13. From the list of licenses, select the license you want to activate.
14. In the table below, click **Activation and Installation**.
The license activation details appear.
15. Click **Extend**.
The **Extend License** window appears.
16. Select **Use an unused license**, and then click **Next**.
The list of unused licenses appears.
17. Select an unused license.




Warning

License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

18. Click **Next**.
19. Click **Browse**.
The file browser appears.
20. Locate and select the DIF from your computer.
21. Click **Upload**.
A confirmation message appears.
22. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
23. Click **Done**.
24. Go back to License Center.
25. In the **License Extension** window, click **Next**.
26. Click **Browse Files**.
The file browser appears.

27. Locate and select the LIF from your computer.
28. Click **Next**.
License Center uploads the LIF and displays the license summary.
29. Click **Extend**.
A confirmation message appears.
30. Click **Close**.
The license appears on the list of active licenses.

Extending a License Offline Using a Product Key

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is about to expire, its status is `Expires soon`.

The **License Extension** window appears.

4. Click **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
A notification message appears.
8. Click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
9. Read and agree to the terms of service.
10. Click **Next**.
11. Read the instructions, and then click **Go to License Manager**.
Your web browser opens the QNAP License Manager website.
12. Sign in with your QNAP ID.
13. Go to **My Licenses**.
14. From the list of licenses, select the license you want to activate.
15. In the table below, click **Activation and Installation**.
The license activation details appear.
16. Click **Extend**.
The **Extend License** window appears.
17. Select **Use a product key**, and then click **Next**.
18. Specify the product key.
19. Click **Next**.

A confirmation message appears.



20. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
21. Click **Done**.
22. Go back to License Center.
23. In the **License Extension** window, click **Next**.
24. Click **Browse Files**.
The file browser appears.
25. Locate and select the LIF from your computer.
26. Click **Next**.
License Center uploads the LIF and displays the license summary.
27. Click **Extend**.
A confirmation message appears.
28. Click **Close**.
The license appears on the list of active licenses.

Upgrading a License

Before upgrading a license, ensure the following.


- The application is already installed on your device.
- You are signed in to myQNAPcloud.

Users can upgrade their existing basic licenses to premium licenses to gain access to advanced features.

1. Open your web browser.
2. Go to <https://software.qnap.com>.
3. Click your account name and select **MY ACCOUNT**.
4. Click **Upgrade Plans**.
A list of upgradable subscriptions is displayed.
5. From the list of subscriptions, find the license you want to upgrade and click **Upgrade**.
The **Current Plan** window appears.
6. From the list of upgrade plans, select an upgrade and click **Add to Cart**.
7. Click .
Click .
8. Click **GO TO CHECKOUT**.
9. Select a payment method.

| Payment Method | User Action |
|----------------|--|
| Credit card | <ul style="list-style-type: none"> a. Specify your card information. b. Verify the items and the price on the order. c. Agree to QNAP terms and conditions. d. Click Place Order. |
| PayPal | <ul style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Pay with PayPal PayPal authentication window appears. d. Specify your PayPal login credentials. e. Click Next. f. Follow PayPal instructions to complete the payment. |
| Google Pay | <ul style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Buy with Google Pay. Google Pay authentication window appears. d. Follow Google Pay instructions to complete the payment. |

10. Apply the license upgrade to your QNAP device.

- a. Open your web browser.
- b. Go to <https://license.qnap.com>.
- c. Sign in with your QNAP ID.
- d. Locate the license from the license list.
- e. Click  .
The **Activate Upgraded License** window appears.
- f. Select **Online Activation**
- g. Click **Next**.
- h. Specify your credentials on the device.
- i. Click **Allow**.
A confirmation message appears.
- j. Click **Close**.

The upgraded license is activated.

Viewing License Information

1. Open your web browser.

2. Go to <https://license.qnap.com>.
3. Sign in with your QNAP ID.
4. View the license information using one of the following modes.

| Viewing Mode | User Actions |
|------------------------|---|
| List by Device | <p>This mode displays all the activated licenses on each device. This allows you to quickly view and manage your licenses on a specific device.</p> <ul style="list-style-type: none"> • Click a device and then click Device Details to view the details of the selected device. • Click a device and then click Activation and Installation to view the details of your licenses. You can also activate or deactivate licenses. |
| List by License | <p>This mode displays your purchased licenses and their details, including available seats, license types, validity period, and status.</p> <ul style="list-style-type: none"> • Click a license and then click License Details to view the details. • Click a license and then click Activation and Installation to view the details. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file. • Click a license and then click Usage Record to view the history of the selected license. |
| List by Product | <p>This mode displays your purchased licenses for each product. This allows you to view and manage all related licenses designed for the same product.</p> <ul style="list-style-type: none"> • Click a product to view the details of your licenses. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file. |

Recovering Licenses

Before recovering licenses, ensure that your device is connected to the internet.


1. Open License Center.
2. Go to **Recover Licenses**.
3. Click **Get Started**.
The **License Recovery** dialog box appears.
4. Read and agree to the terms of service.
5. Click **Recovery**.
License Center automatically recovers all available licenses for applications installed on your devices.

Transferring a License to the New QNAP License Server

This task only applies to existing licenses that have been activated using PAK.

Before transferring licenses, ensure the following.

- Your NAS is connected to the internet.

- You are signed in to myQNAPcloud.
1. Open License Center.
 2. Go to **My Licenses**.
 3. Identify the license you want to transfer, and then click .
A confirmation message appears.
 4. Read the terms of service, and then click **Transfer & Activate**.

**Warning**


After you register a license with your current QNAP ID, it will no longer be transferable.

License Center transfers the license.
A confirmation message appears.

5. Optional: Click **QNAP License Manager** to review the license details.
6. Click **Close**.

Deleting a License

Before deleting a license, ensure that you have deactivated this license.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to delete, and then click .
A confirmation message appears.
4. Click **Yes**.
License Center deletes the license.

**Tip**

If the license has not yet expired, the license will still be listed in the **License Activation** table.

15. Multimedia

QTS provides a range of applications and utilities for viewing, playing, and streaming multimedia files stored on the NAS.

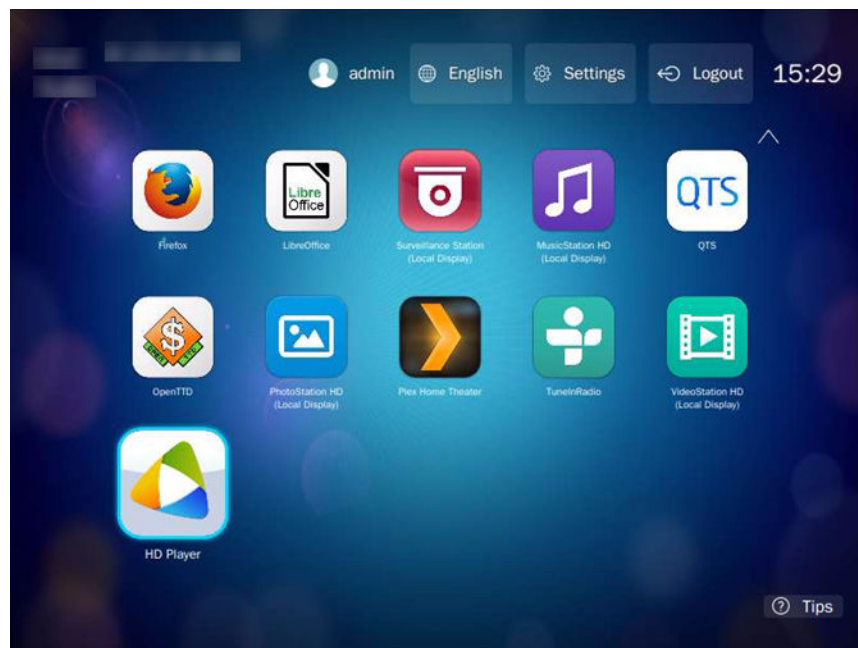
| Application/Utility | Description |
|---------------------------------|--|
| HybridDesk Station (HD Station) | Connect to an HDMI display to access multimedia content on your NAS. |
| DLNA Media Server | Configure your NAS as a Digital Living Network Alliance (DLNA) server to access media files on your NAS from devices on your home network. |
| Media Streaming Add-on | Stream media from your NAS to DLNA, Chromecast, and HDMI-connected devices. |
| Multimedia Console | Manage multimedia apps and content on the NAS. You can index files, transcode videos, and generate thumbnails for multimedia content. |

HybridDesk Station (HD Station)

HybridDesk Station (HD Station) allows you to connect to an HDMI display and directly access multimedia content and use other applications on your NAS. You can use your NAS as a home theater, multimedia player, or desktop substitute. After installing HD Station and connecting the NAS to an HDMI display, you can navigate your NAS using HD Station.


HD Station requires:

- A TV or monitor with an HDMI port
- A mouse, keyboard, or remote control for navigation
- A graphics card (some NAS models only). Go to <https://www.qnap.com> to check the software specifications for your NAS and verify that it is compatible with HD Station.



Installing HD Station

1. Go to **Control Panel > Applications > HDMI Display Applications** .
2. Choose one of the following installation methods.

| Installation Method | Steps |
|---------------------|--|
| Guided installation | <ol style="list-style-type: none"> a. Click Get Started Now. The HybridDesk Station window appears. b. Review the list of selected applications. <p> Tip All applications are selected by default. You can deselect applications that you do not want to install.</p> <ol style="list-style-type: none"> c. Click Apply. |
| Manual installation | <ol style="list-style-type: none"> a. Under Install Manually, click Browse. b. Select HD Station. c. Click Install. |

QTS installs HD Station and the selected applications.







Note

Multimedia Services must be enabled to play multimedia content in HD Station. Go to **Main Menu > Applications > Multimedia Console** to enable Multimedia Services. HD Player, Photo Station, Music Station, and Video Station must also be installed on the NAS to play multimedia content from the respective applications.

Configuring HD Station

1. Go to **Control Panel > Applications > HDMI Display Applications > Local Display settings** .
2. Perform any of the following actions.

| Action | Steps |
|--|---|
| Enable HD Station | <p>Click Enable.</p> <p> Note HD Station must be disabled to perform this action.</p> |
| Disable HD Station | <p>Click Disable.</p> <p> Note HD Station must be enabled to perform this action.</p> |
| Install all HD Station applications | <p>a. Click Install All Apps. A dialog box appears.</p> <p>b. Click OK.</p> |
| Update installed apps | Click Update . |
| Restart HD Station | Click Restart . |
| Remove HD Station and related applications | <p>a. Click Remove. A dialog box appears.</p> <p>b. Click OK.</p> |
| Edit HD Station settings | <p>a. Click Settings. The Settings window appears.</p> <p>b. Modify any of the following settings:</p> <ul style="list-style-type: none"> • Output resolution: Change the resolution of HD Station. • Overscan: Reduce the visible area of a video displayed in HD Station. • Enable Remote Desktop: View the NAS HDMI output using your web browser. <p> Note</p> <ul style="list-style-type: none"> • Enabling Remote Desktop may affect the playback quality of local videos. • You must restart Remote Desktop after changing the output resolution. <p> Tip You can also open and restart Remote Desktop from this screen.</p> |
| Install HD Station apps | <p>a. Under Install Manually, click Browse.</p> <p>b. Select the application.</p> <p>c. Click Install.</p> |

HD Station Applications

Go to **App Center > HybridDesk Station** to install or configure applications used with HD Station.

Using HD Player in HD Station

You can use HD Player to browse and play multimedia content in Photo Station, Music Station, and Video Station.

1. Connect an HDMI display to the NAS.
2. Select your NAS account.
3. Specify your password.
4. Start HD Player.
5. Select your NAS account.
6. Specify your password.

HDMI Local Display and DLNA Media Server

You can stream multimedia content to High-Definition Multimedia Interface (HDMI) display applications or Digital Living Network Alliance (DLNA) devices. These services require you to enable Multimedia Services. To enable Multimedia Services, go to **Control Panel > Applications > Multimedia Console > Overview**.

Enabling HDMI Display Applications

1. Log on to QTS as administrator.
2. Go to **Control Panel > Applications > HDMI Display Applications**.
3. Locate the application you want to enable.
4. Optional: Configure the following settings.
 - a. Click **Settings**.
 - b. Configure the application settings.



Note

You may be required to update an application, connect a monitor, display to the NAS before successfully applying the settings.

- c. Click **Apply**.
5. Click **Enable**.
A confirmation window appears.



Note

A confirmation window only appears if you have another application enabled.

6. Click **OK**.
QTS enables the application.

Enabling DLNA Media Server

You can configure your NAS as a DLNA server, allowing you to access media files on your NAS through your home network using DLNA devices such as TVs, smartphones, and computers.

The contents displayed in DLNA Media Server are based on user account permissions and Multimedia Console settings.



Important

The first time you enable DLNA Media Server, QTS automatically installs the Media Streaming Add-on if it is not already installed on the NAS. For details, see [Media Streaming Add-on](#).


1. Go to **Control Panel > Applications > DLNA Media Server**.
2. Select **Enable DLNA Media Server**.
3. Optional: Specify the following information.

| Field | Description |
|------------------------------------|---|
| Service Name | Specify a name for the DLNA Media Server. |
| Select default user account | Select the user account that will be the directory for the DLNA Media Server. |

4. Click **Apply**.

Configuring DLNA Media Server

1. Go to **Control Panel > Applications > DLNA Media Server**.
2. Perform any of the following actions.

| Action | Steps |
|-----------------------------|--|
| Scan for multimedia content | Click Scan now . |
| Restart DLNA Media Server | Click Restart . |
| Configure advanced settings | <ol style="list-style-type: none"> a. Click Advanced Settings. The Media Streaming Add-on portal opens in a new browser window. b. Configure the settings. <div style="margin-top: 10px;">  <p>Note Media Streaming Add-on must be installed to configure advanced settings. For details, see Media Streaming Add-on.</p> </div> |

Media Streaming Add-on

Media Streaming Add-on allows you to stream media from your NAS to different DLNA, Chromecast, and HDMI-connected devices simultaneously using the following QTS multimedia applications:

- File Station
- Photo Station

- Music Station
- Video Station

Go to App Center to install Media Streaming Add-on.



Tip

You can restart Media Streaming Add-on anytime by clicking **Restart** on the home screen.

The screenshot shows the 'Media Streaming Add-on' configuration page. On the left is a sidebar with 'General Settings', 'Browsing Settings', and 'Media Receivers'. The main content area includes a 'Restart' button, a 'Please note' box, and a settings form. The form fields are: Service name (TW-TEST1), Default user account (admin), Network interface (automatic), Port (8200), Menu language (English), and Default menu style (Simple). An 'Apply All' button is located at the bottom of the settings area.

Configuring General Settings

1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.




Note

Media Streaming Add-on logs you in based on your QTS user credentials. If a login screen appears, you will need to specify your username and password to log in.

2. Go to **General Settings**.
3. Modify any of the following settings.

| Setting | Description |
|-----------------------------|--|
| Service name | This is the name that devices on the local network will see when connecting to the NAS. |
| Default user account | Select the user account that media devices receive content from. To connect using a different user account, you must specify the account's username and password in the connection settings of the media receiver. |
| Network interface | Select the network interface. |
| Port | Specify the port number. |
| Menu language | Select the language displayed for menu items. |

| Setting | Description |
|---|---|
| Default menu style | Select the type of menu style. <ul style="list-style-type: none"> • Simple • All categories • Custom Select one of the Custom options and click Customize to configure the display options for the menu. |
| Always stream videos to Apple TV and Chromecast in original file formats | When selected, the NAS streams videos to these devices without transcoding or embedding subtitles. <p> Important Ensure that Apple TV and Chromecast support the file formats of videos on your NAS when selecting this option.</p> |

4. Click **Apply All**.

Configuring Browsing Settings

1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.



Note

Media Streaming Add-on logs you in based on your QTS user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Browsing Settings**.
3. Modify any of the following settings.

| Setting | Description |
|----------------------------------|---|
| Display Photo | Select the display size of the thumbnail for photo albums. |
| Music title display style | Select the type of information that is displayed for music files. |
| Video title display style | Select whether video titles display the file name of the video or the embedded information. |

4. Click **Apply All**.

Configuring Media Receivers

1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.



Note

Media Streaming Add-on logs you in based on your QTS user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Media Receivers**.
3. Perform any of the following actions.

| Action | Steps |
|---------------------------|--|
| Enable device sharing | Select Enable sharing for new media receivers automatically . When enabled, newly discovered devices will automatically be allowed to connect to DLNA Media Server. |
| Scan for new devices | Click Scan for devices Media Streaming Add-on searches for new media devices connected to the NAS. |
| Modify device connections | Select or deselect media devices. Only selected devices can connect to DLNA Media Server. |

4. Click **Apply All**.

Multimedia Console

Multimedia Console helps you manage installed multimedia apps and content stored on the NAS. Multimedia Console can index files, transcode videos, and generate thumbnails for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Server.

Overview

The **Overview** screen displays the indexing and thumbnail generation status for multimedia files as well as the total number of photos, videos, and music files on your NAS



Important

To use third-party applications and Multimedia Console features like indexing and thumbnail generation, Multimedia Services must be enabled.



Tip

You can enable or disable Multimedia Services in the upper right of the **Overview** screen.

Multimedia Console

Multimedia Console

Multimedia Services: **Enabled**

Overview

Status
Monitor indexing and thumbnail generation for multimedia content.

Index

Completed

Last update: 2018/11/07 11:23:27
Total files: 1808

Thumbnail

Completed

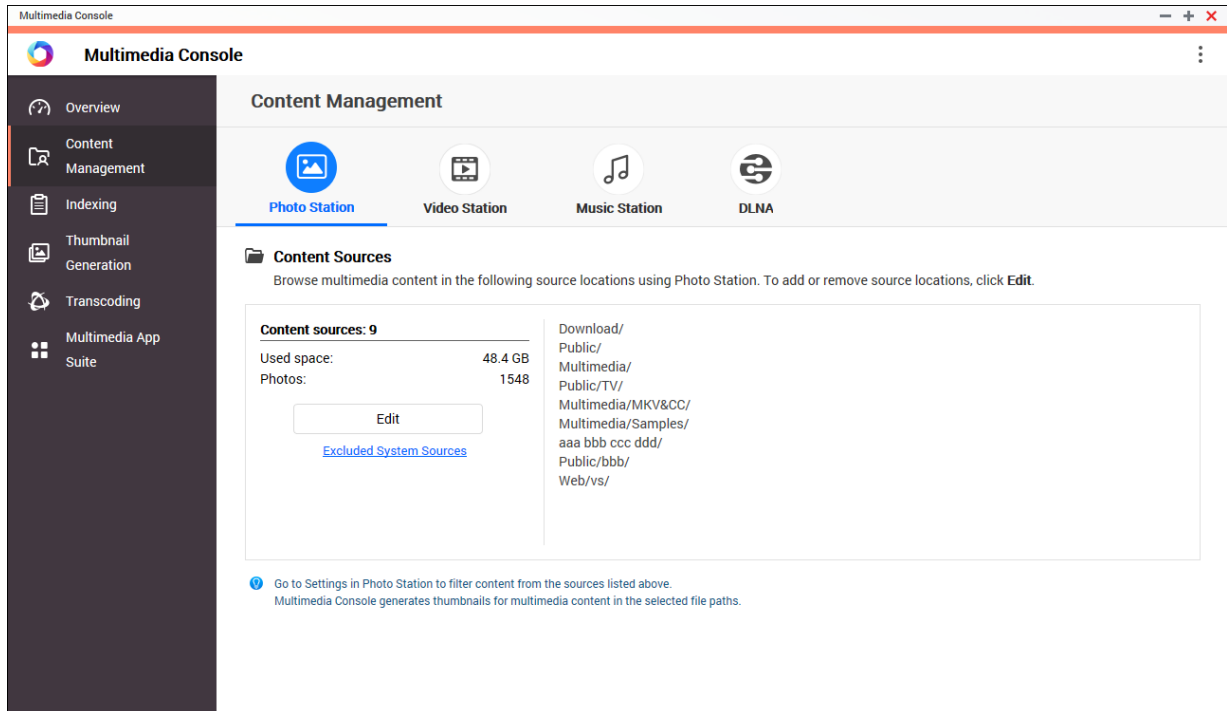
Last update: 2018/11/05 09:48:18
Total files: 1808

Content Information
View contents and the five most frequently used tags.

| Contents | Photo | Video | Music |
|--------------|--------------------------|-----------------|--------------------------|
| Photos: 1550 | Photo 1 | TV_test_1025 23 | QNAP Samp... 2 |
| Videos: 253 | Add tags | Movies 11 | bbb 1 |
| Music: 5 | | tv_test_123 3 | ccc 1 |
| | | TV Shows 1 | Add tags |

Content Management

The **Content Management** screen displays the content source folders for multimedia apps installed on the NAS. You can view and edit the content source folders for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Media Server.



Editing Content Sources

1. Open Multimedia Console.
2. Go to **Content Management**.
3. Select an app or service.
4. Click **Edit**.
The **Edit Content Sources** window appears.
5. Select or deselect content source folders.
The **Selected Folder Paths** list updates.
6. Click **Apply**.

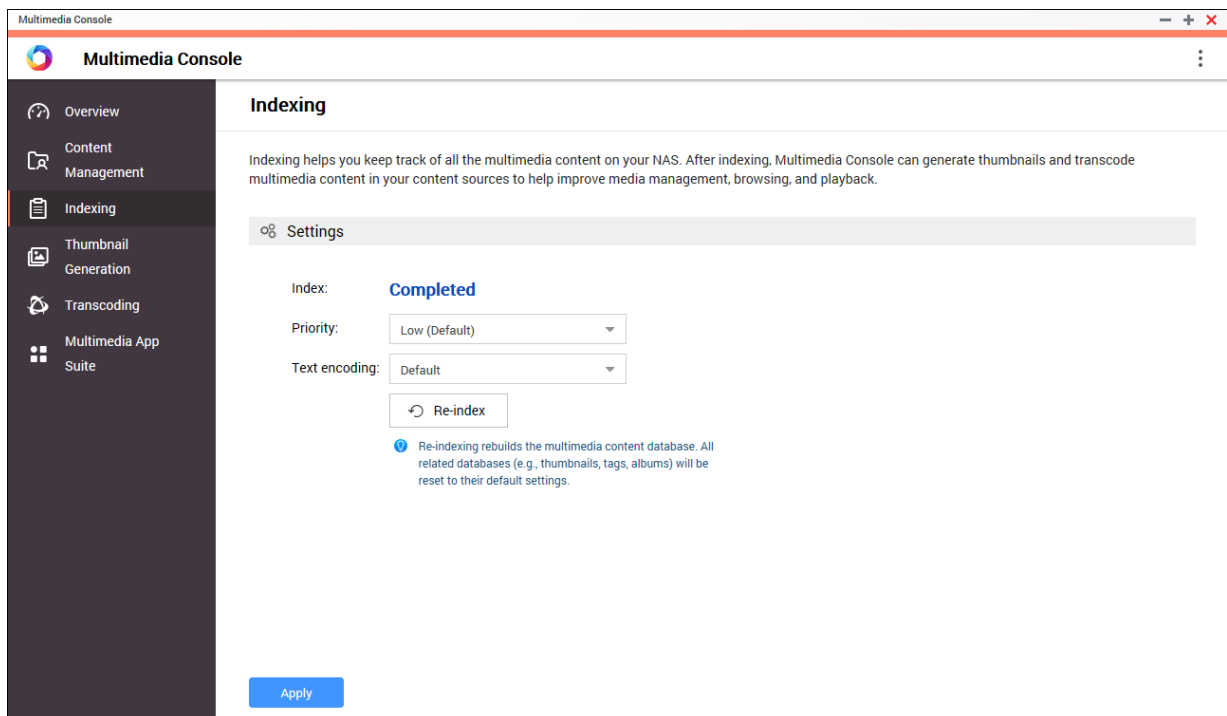


Tip

Click **Excluded System Sources** on the **Content Management** screen to view system folder paths that are excluded from Multimedia Services.

Indexing

Multimedia Console improves content management, browsing, and playback when accessing files in various multimedia apps by scanning and indexing multimedia files on your NAS.



Configuring Indexing Settings

1. Open Multimedia Console.
2. Go to **Indexing**.
3. Select the **Priority**.
 - **Low (Default)**
 - **Normal**

The **Priority** determines the amount of system resources allocated to the indexing process.

4. Select the type of **Text encoding**.
The type of **Text encoding** determines the character encoding scheme that Multimedia Console uses to index text and data in your multimedia files. The default encoding scheme is Unicode.
5. Click **Apply**.



Tip

Click **Re-index** to rebuild the multimedia content database and revert dependent databases to their default settings.

Thumbnail Generation

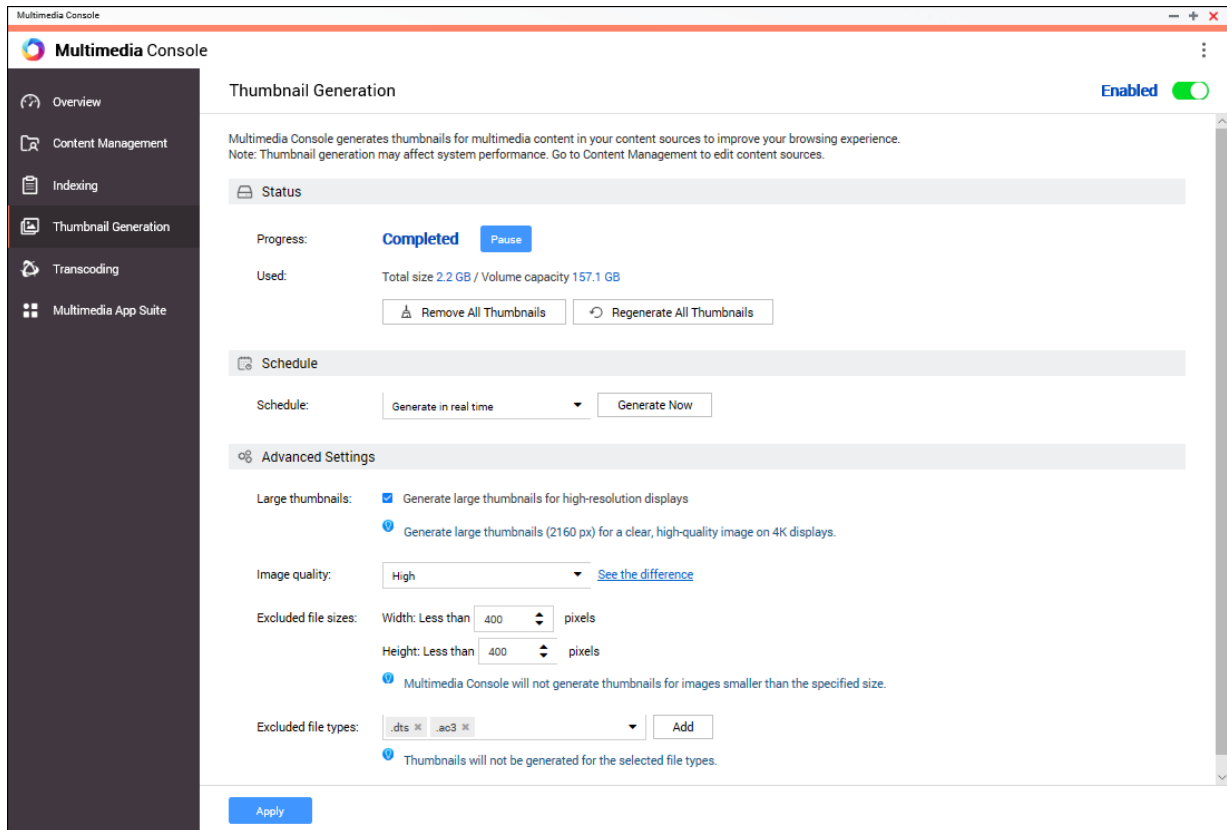
Multimedia Console generates thumbnails for multimedia files to improve browsing.



Note


- Thumbnail generation is enabled by default if Multimedia Services is enabled.


- You can disable thumbnail generation in the upper right of the **Thumbnail Generation** screen.
- Generating thumbnails may affect system performance.



Configuring Status


1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Status**.
3. Perform any of the following tasks.

| Task | Steps |
|----------------------------|---|
| Pause thumbnail generation | <ol style="list-style-type: none"> Next to Progress, click Pause. The Pause window opens. Select Pause. Click OK. <p> Tip Click Resume when thumbnail generation is paused to resume thumbnail generation.</p> |

| Task | Steps |
|-------------------------------|--|
| Postpone thumbnail generation | <p>a. Next to Progress, click Pause. The Pause window opens.</p> <p>b. Select Postpone.</p> <p style="padding-left: 20px;">1. Select the duration.</p> <p>c. Click OK.</p> <p> Tip Click Resume when thumbnail generation is postponed to resume thumbnail generation.</p> |
| Remove thumbnails | <p>a. Under Used, click Remove All Thumbnails. A dialog box appears.</p> <p>b. Click OK.</p> |
| Regenerate thumbnails | <p>a. Under Used, click Regenerate All Thumbnails. A dialog box appears.</p> <p>b. Click OK.</p> |

Configuring Schedule

1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Schedule**.
3. Next to **Schedule**, select one of the following options.

| Option | Description |
|--------------------------------|---|
| Generate in real time | Multimedia Console generates thumbnails for new files as soon as they are detected. |
| Generate using schedule | <p>Multimedia Console generates thumbnails according to a specified schedule.</p> <p> Note When selected, you must specify a thumbnail generation schedule.</p> |
| Generate manually | Multimedia Console generates thumbnails only after clicking Generate Now . |




Tip

Click **Generate Now** to force Multimedia Console to start generating thumbnails immediately.

4. Click **Apply**.

Configuring Advanced Settings

1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Advanced Settings**.
3. Configure any of the following settings.

| Setting | Description |
|----------------------------|--|
| Large thumbnails | When selected, Multimedia Console generates high-resolution thumbnails (2160 px) for media files. |
| Image quality | Select High or Low .  Tip Click See the difference to view a side-by-side comparison of high- and low-quality thumbnails. |
| Excluded file sizes | Multimedia Console only generates thumbnails for images that are larger than the specified resolution. |
| Excluded file types | Multimedia Console will not generate thumbnails for the selected file types. |

4. Click **Apply**.

Transcoding

The transcoding feature in Multimedia Console converts video files to MPEG-4 format for improved compatibility with media players on mobile devices, smart TVs, and web browsers. Transcoding can also scale down the resolution of video files to prevent buffering in slower network environments.

You can create and manage transcoding tasks and configure settings from the **Transcoding** screen in Multimedia Console.

Overview

You can manage Background Transcoding and On-the-Fly Transcoding tasks from the Overview tab on the **Transcoding** screen.



Note

- Transcoding is only available for certain NAS models. Go to <https://www.qnap.com/en/compatibility> to view specifications for your NAS and verify that it is compatible.
- Transcoding uses additional NAS storage space to store transcoded files.

| Type | Description |
|-------------------------------|--|
| Background Transcoding | Background Transcoding converts videos asynchronously to minimize consumption of system resources if the video is accessed by multiple users simultaneously. You can manually add videos to background transcoding folders using File Station, Photo Station, or Video Station. For details on managing background transcoding folders, see Configuring Background Transcoding Folders . |

| Type | Description |
|-------------------------------|--|
| On-the-Fly Transcoding | <p>On-the-Fly Transcoding converts videos in real time as you watch them.</p> <p>Note</p> <ul style="list-style-type: none"> You cannot specify the output format for On-the-Fly Transcoding. On-the-Fly Transcoding uses more system resources than Background Transcoding and may affect the performance of your NAS. <p>Tip</p> <p>You can install CodexPack to increase transcoding speed and reduce system resource consumption. You can check whether your NAS supports GPU-accelerated transcoding on the Transcoding Settings screen. For details, see Configuring Transcoding Resources.</p> |

Background Transcoding

The Background Transcoding tab displays the overall background transcoding status as well as additional information about specific background transcoding tasks. You can view and manage background transcoding tasks from this tab.

Multimedia Console

Multimedia Console

Overview

Content Management

Indexing

Thumbnail Generation

Transcoding

Multimedia App Suite

Transcoding

Convert various video formats to MPEG-4 to improve compatibility when using other browsers or devices.

Overview Settings

Background Transcoding On-the-fly Transcoding

Transcoding status: **Transcoding...** Pause



Incomplete Remove All Incomplete Tasks Remove All Completed Tasks

| File Name | Size/Durat. | Output Format | Time (Start/Finish) | Status | Transcoding Method | Actions |
|------------------------------|----------------------|---------------|----------------------|--------------------|--------------------|---------|
| lion-sample.mov | 10.3 MB 00:01:56 | 1080p | 2019/01/31 12:23:... | Transcoding... 37% | CPU | 📄 🗑️ |
| POCAWE_Sample.mkv | 237.9 MB 00:01:00 | Original | -- | Standby | -- | 📄 🗑️ |
| jellyfish-25-mbps-hd-hevc... | 13.7 MB 00:00:30 | Original | -- | Standby | -- | 📄 🗑️ |




Page 1 / 1

Display item: 1 - 3, Total: 3 Show 10 Item(s)

General Tasks

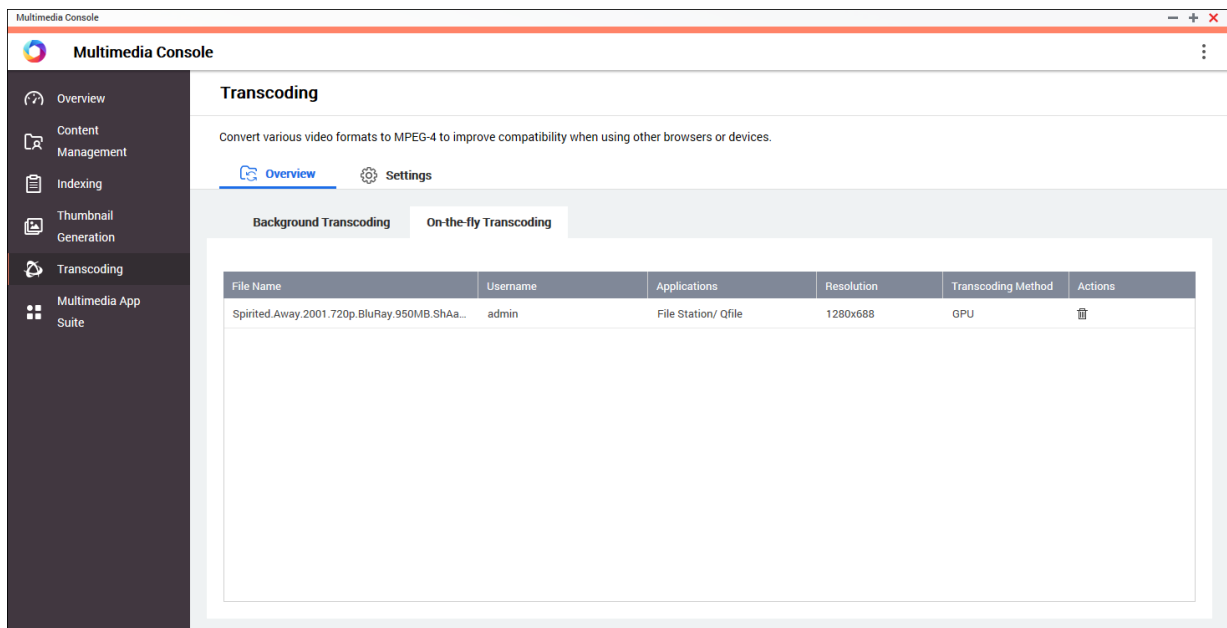
| Task | User Action |
|---------------------------------|--|
| Pause background transcoding | <ol style="list-style-type: none"> 1. Click Pause. The Pause window opens. 2. Select Pause. 3. Click OK. <p> Tip Click Resume when background transcoding is paused to resume background transcoding.</p> |
| Postpone background transcoding | <ol style="list-style-type: none"> 1. Click Pause. The Pause window opens. 2. Select Postpone. <ol style="list-style-type: none"> a. Select the duration. 3. Click OK. <p> Tip Click Resume when background transcoding is postponed to resume background transcoding.</p> |
| View completed tasks | Above the background transcoding task table, select Completed from the drop-down list. Multimedia Console displays completed background transcoding tasks. |
| View incomplete tasks | Above the background transcoding task table, select Incomplete from the drop-down list. Multimedia Console displays incomplete background transcoding tasks. |
| Remove incomplete tasks | <ol style="list-style-type: none"> 1. Click Remove All Incomplete Tasks. A dialog box appears. 2. Click OK. |
| Remove completed tasks | <ol style="list-style-type: none"> 1. Click Remove All Completed Tasks. A dialog box appears. 2. Click OK. |


Task Table Configuration (Incomplete Tasks)

| Button | Description |
|---|---|
|  | Moves a task up in the list and increases its priority. |
|  | Moves a task down in the list and decreases its priority. |
|  | Removes a task from the list. |

On-the-fly Transcoding

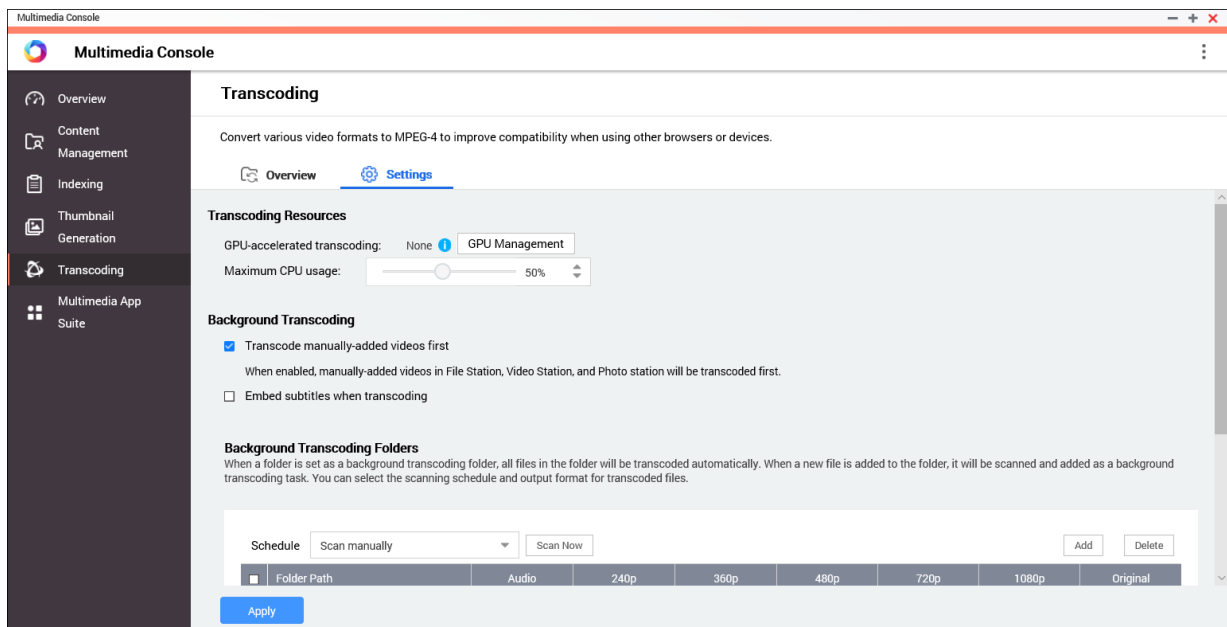
The On-the-Fly Transcoding tab displays information about on-the-fly transcoding tasks. You can view and manage on-the-fly transcoding tasks from this tab.



Tip
Click  to remove a task from the list.

Settings

You can manage Background Transcoding and On-the-Fly Transcoding settings from the Settings tab on the **Transcoding** screen.



Configuring Transcoding Resources

1. Open Multimedia Console.

2. Go to **Transcoding > Settings > Transcoding Resources** .
3. Optional: Enable **GPU-accelerated transcoding**.
 - a. Click **GPU Management**.
The **System > Hardware > Graphics Card** screen appears.
 - b. Configure graphics card settings.
For details, see [Configuring Hardware Resource Settings](#).
4. Specify the **Maximum CPU usage** allocated to transcoding tasks.
5. Click **Apply**.

Configuring Background Transcoding Settings


1. Open Multimedia Console.
2. Go to **Transcoding > Settings > Background Transcoding** .
3. Configure any of the following settings.


| Setting | Description |
|--|--|
| Transcode manually-added videos first | Videos in File Station, Video Station, and Photo Station that are manually added will be transcoded first. |
| Embed subtitles when transcoding | Multimedia Console automatically embeds subtitles to videos when transcoding them. |

4. Click **Apply**.

Configuring Background Transcoding Folders

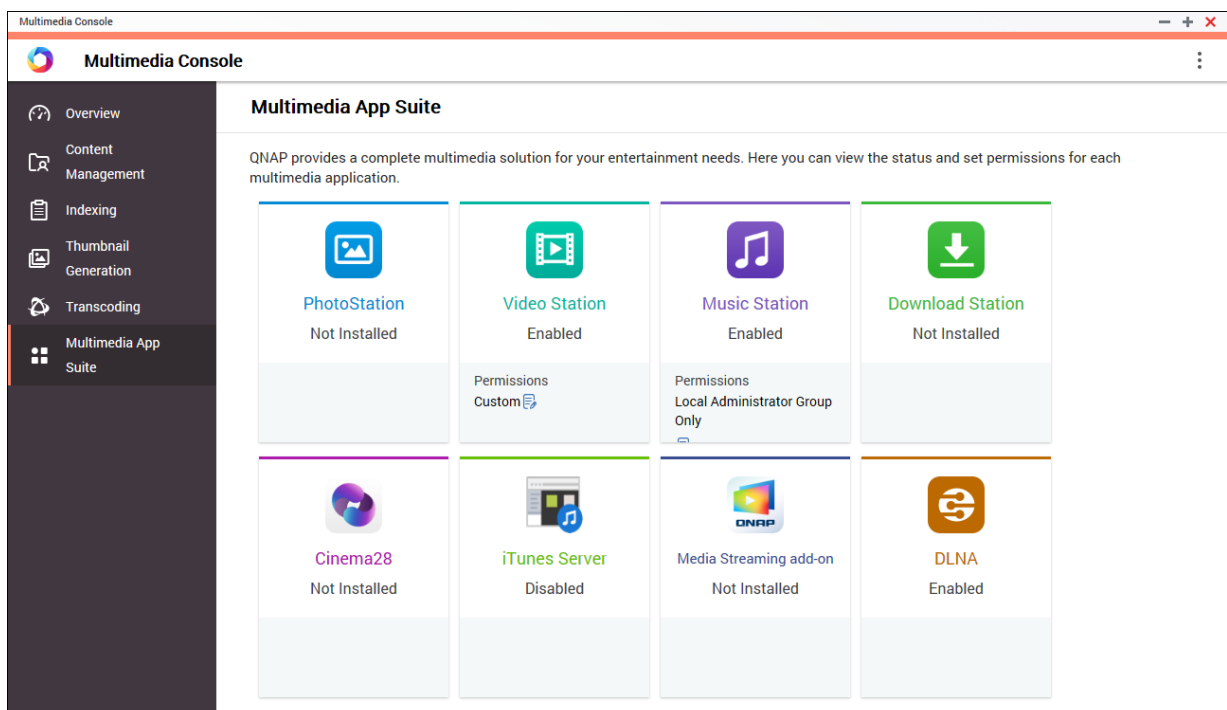
1. Open Multimedia Console.
2. Go to **Transcoding > Settings > Background Transcoding Folders** .
3. Perform any of the following tasks.

| Task | User Action |
|--|--|
| Configure the scanning schedule for background transcoding folders | <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Scan in real time: Multimedia Console scans background transcoding folders for new files and adds the files as background transcoding tasks as soon as they are detected. • Scan using schedule: Multimedia Console scans background transcoding folders for files according to a specified schedule. <p> Note When selected, you must specify the time of day that Multimedia Console generates thumbnails.</p> <ul style="list-style-type: none"> • Scan manually: Multimedia Console scans background transcoding folders only when you click Scan Now. |

| Task | User Action |
|--|---|
| Add a background transcoding folder | <p>a. Click Add. The Add Background Transcoding Folders window appears.</p> <p>b. Select a folder.</p> <p>c. Specify the output format.</p> <p>d. Click Apply.</p> |
| Remove a background transcoding folder | <p>a. Select a background transcoding folder.</p> <p>b. Click Delete.</p> |
| Configure transcoding output format | <p>a. Locate a background transcoding folder on the list.</p> <p>b. Select the output format.</p> <p> Note Multimedia Console upscales the video if the selected resolution is higher than the original resolution of the video.</p> <p>c. Click Apply.</p> |

Multimedia App Suite

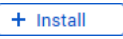
You can view statuses and configure user and group access permissions for installed multimedia apps and services from the **Multimedia App Suite** screen.



Configuring Multimedia Apps and Services

1. Open Multimedia Console.

2. Go to **Multimedia App Suite**.
3. Perform any of the following tasks.

| Task | User Action |
|---------------------------|---|
| Install an app or service | <ol style="list-style-type: none"> a. Locate an app or service with the status Not Installed under the app or service name. b. Click Not Installed. The App Center and app installation windows open. c. Click . |
| Enable an app or service | <ol style="list-style-type: none"> a. Locate an app or service with the status Disabled under the app or service name. b. Click Disabled. c. The app or service opens in a new window. d. Enable the app or service. |
| Disable an app or service | <ol style="list-style-type: none"> a. Locate an app or service with the status Enabled under the app or service name. b. Click Enabled. c. The app or service opens in a new window. d. Disable the app or service. |

Configuring Multimedia App Permissions



1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.
3. Locate an app with access permissions.
4. Under **Permissions**, click the permission status.
The **Permission Settings** window opens.
5. Select a permission type.

| Permission Type | Description |
|---------------------------------------|---|
| All Users | All users can access the app. |
| Local Administrator Group Only | Only users in the local administrator group can access the app. |
| Custom | Specified users and user groups can access the app. |

A dialog box appears.

6. Click **OK**.
7. Perform any of the following actions.

| Permission Type | User Action |
|------------------|----------------------|
| All Users | Click Close . |

| Permission Type | User Action |
|---------------------------------------|---|
| Local Administrator Group Only | Click Close . |
| Custom | <p>a. Select a user or user group type:</p> <ul style="list-style-type: none"> • Local • Domain <p>b. Choose to deny or allow access to selected users or groups. A dialog box appears.</p> <ol style="list-style-type: none"> 1. Click OK. <p>c. Filter the list by users or groups.</p> <p> Tip Use the Search field to quickly find users or groups.</p> <p>d. Select a user or group.</p> <p>e. Click Add. The user or group is added to the Selected Users/Groups list.</p> <p> Tip</p> <ul style="list-style-type: none"> • Select a user or group and click Delete to remove the user or group from the list. • Click Delete All to remove all users or groups from the list. <p>f. Click Save.</p> <p>g. Click Close.</p> |

Installing and Managing AI Engines

1. Install QuMagie Core.
For details, see [Installing an App from App Center](#).



Note

This process can take a while.


2. Open Multimedia Console.
3. Select **AI Engines**.



Tip

- QuMagie Core supports Google TPU devices. To check if the Google TPU device is successfully running on the NAS, go to **Control Panel > System > Hardware > Hardware Resources**.
- You can check the status of the Google TPU device on the top right corner of the screen. If QuMagie Core is running the Google TPU device, the status changes to **Google TPU: Running**. If the Google TPU device is not running, the status changes to **Google TPU: Stopped**.

4. Locate an AI engine you want to manage and select one of the following options.

| Option | User Action |
|----------------|---|
| Pause | <p>a. Click Pause. The Pause window opens.</p> <p>b. Select one of the following options.</p> <ul style="list-style-type: none"> • Pause: Pauses the engine now. • Postpone: Pauses the engine after a specific time period. <p> Note You can postpone by 1, 2, or 5 hours.</p> <p>c. Click OK.</p> |
| Restart | <p>a. Click Restart. A confirmation message appears.</p> <p>b. Click OK.</p> |

QuMagie Core pauses or restarts the AI engine.

16. QuLog Center

QuLog Center allows you to centrally manage and monitor logs from local devices and remote devices. You can specify log filters, create notification rules, and configure log settings to stay informed of your device status and important events. You can view and manage system logs in **Control Panel > System > QuLog Center**.

Monitoring System Logs

The **Overview** screen provides statistical graphics to help you visualize system log data and monitor device status.

System Event Log

The **System Event Log** tab provides the following widgets to visualize the statistical data of the system event logs from your devices.




Important

You must configure a log destination to enable the system event log feature. For details, see [Configuring Event Log Settings](#).



Tip

The System Event Log page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

| Widget | Description |
|--|--|
| Logs Over Time | <p>This widget displays a line chart to visualize the number of log entries over time.</p> <div style="border-left: 2px solid #ffc107; padding-left: 10px; margin-top: 10px;"> <p>Tip</p> <ul style="list-style-type: none"> • Click  to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time. </div> |
| Top 5 Applications for Error Logs | This widget displays the five applications that have the largest numbers of error log entries. |
| Top 5 Applications for Warning Logs | This widget displays the five applications that have the largest numbers of warning log entries. |



Monitoring System Access Logs

The **System Access Log** tab provides the following widgets to visualize the statistical data of the system access logs from your devices.



Tip

The System Access Log page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

| Section | Description |
|-------------------------|---|
| Logs Over Time | <p>This widget displays a line chart to visualize the number of log entries over time.</p> <p> Tip</p> <ul style="list-style-type: none"> • Click  to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time. |
| Currently Online | This widget lists the current online users and provides the information of their user sessions. |
| Connection Types | This widget displays a pie chart to visualize the numbers of user sessions for each communication protocol. |
| Logged in | This widget displays a pie chart to visualize the numbers of successful logins using each IP address or user account. |
| Failed to log in | This widget displays a pie chart to visualize the numbers of failed login attempts using each IP address or user account. |

Local Logs

Local Device Logs allows you to monitor system event logs, system access logs, and online user status on one local device. You can also configure log filters, log settings, and remove event indicators.

Local System Event Logs


You can monitor and manage system event logs from local devices in **Local Device > System Event Log**.














Important

You must configure a log destination to enable the local system event log feature. For details, see [Configuring Event Log Settings](#).

On the **System Event Log** screen, you can perform the following tasks:

| Task | Steps |
|---------------------|---|
| Select a group mode | <ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By app: this mode groups log entries by app name. • By date: this mode groups log entries by date. • By content: this mode groups log entries by log content. • By user: this mode groups log entries by users. • By Source IP: this mode groups log entries by source IP address. |

| Task | Steps |
|------------------------|--|
| Select a display style | <ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click Add Style to create a display style. For details, see Configuring Display Settings.</p> |
| Export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 7. Click Export. |
| Download export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer. |

| Task | Steps |
|-----------------------------------|---|
| Perform a search | <ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for System Event Log. |
| Select display items | <ol style="list-style-type: none"> 1. Click . 2. Select the items to display. |
| Create an event notification rule | <p>You can quickly create an event notification rule using a log entry. This allows you to receive notifications for events similar to the selected log entry.</p> <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event notification rule. Notification Center opens and the Create event notification rule windows appears. For details, see Creating an Event Notification Rule. |
| Create an event flag rule | <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event flag rule. The Create Event Flag Rule window appears. 4. Click Create. The event is flagged. Go to Log Settings > Event Indicators to view all event flags. |
| Select all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all. |
| Deselect all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection. |
| Copy one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . <p>The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.</p> |
| Delete one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . <p>A confirmation message appears.</p> <ol style="list-style-type: none"> 3. Click Yes. |

Local System Access Logs

You can monitor and manage system access logs from local devices in **Local Device > System Access Log**.








Important

You must configure a log destination to enable the system access logs feature. For details, see [Configuring Local System Access Logs](#).

On the **System Access Log** screen, you can perform the following tasks:

| Task | Steps |
|------------------------|--|
| Select a group mode | <ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By date: this mode groups log entries by date. • By user: this mode groups log entries by user. • By source IP: this mode groups log entries by source IP address. |
| Select a display style | <ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click Add Style to create a display style. For details, see Configuring Display Settings.</p> |
| Export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> 4. Select the maximum number of log entries per file. 5. Compress the export file and specify a password. 6. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 7. Click Export. |

| Task | Steps |
|--------------------------------|---|
| Download export logs | <ol style="list-style-type: none"> 1. Click  . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer. |
| Perform a search | <ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for Local System Access Log. |
| Select display items | <ol style="list-style-type: none"> 1. Click  . 2. Select the items to display. |
| Select all log entries | <ol style="list-style-type: none"> 1. Select one log entry. 2. Click Select multiple entries. The Select multiple entries drop-down menu appears. 3. Click Select all . All log entries are selected. |
| Deselect all log entries | <ol style="list-style-type: none"> 1. Select one log entry. 2. Click Select multiple entries. The Select multiple entries drop-down menu appears. 3. Click Invert selection . All log entries are deselected. |
| Copy one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click  . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere. |
| Delete one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click  . A confirmation message appears. 3. Click Yes. |

| Task | Steps |
|---|---|
| Add one or more log entry to the block list | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click Add to block list. The Add to block list drop-down menu appears. 3. Select a block period option. |

Viewing Online Users

On the **Online Users** screen, you can see the list of online users and their detailed information, such as login date, login time, username, source IP address, and connection type.

You can perform the following tasks:

| Tasks | Steps |
|--|---|
| Remove a connection | <ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Disconnect. A confirmation message appears. 4. Click Yes. |
| Block a user | <ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Add to block list. 4. Select a block period option. |
| Remove the connection and block the user | <ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Disconnect and add to a block list. A confirmation message appears. 4. Select a block period option. |
| Select the items to display on the list | <ol style="list-style-type: none"> 1. Click +. 2. Select the items to display. |


Creating a Custom Filter Tab for Local Device System Logs








You can create custom filter tabs for Local System Event Logs, Local System Access Logs, and Online Users. The customized filter tabs can filter logs or user information based on specified keywords or criteria. For details, see the following topics:

- [Creating a Custom Filter Tab for System Event Logs](#)
- [Creating a Custom Filter Tab for Local System Access Logs](#)

Creating a Custom Filter Tab for System Event Log

1. Open QuLog Center.


2. Go to **Local Device > System Event Log** .
3. Go to the search bar.
4. Click  .
The **Advanced Search** window appears.
5. Specify the following filter fields:







| Fields | Steps |
|-----------------------|---|
| Severity Level | <ol style="list-style-type: none"> a. Click  . The severity level drop-down menu appears. b. Select a severity level option. |
| Application | <ol style="list-style-type: none"> a. Click  . The application drop-down menu appears. b. Select an application. The Category option appears. <div style="border-left: 2px solid #0070c0; padding-left: 10px; margin-top: 10px;"> <p> Note The Category option only appears when you specify the application.</p> </div> <ol style="list-style-type: none"> c. Specify the application Category. |
| Date | <ol style="list-style-type: none"> a. Click  . The date drop-down menu appears. b. Select a date option. |
| Content | <ol style="list-style-type: none"> a. Click  . The content condition option appears. b. Select a condition. c. Specify the content keywords. |
| User | <ol style="list-style-type: none"> a. Click  . The user condition option appears. b. Select a condition. c. Specify the keywords. |
| Source IP | <ol style="list-style-type: none"> a. Click  . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address. |


6. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
7. Click **Search**.
The list of filtered results is displayed.

8. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.
9. Enter a tab name.
10. Click **Apply**.
 - The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.

Creating a Custom Filter Tab for Local System Access Log

1. Open QuLog Center.
2. Go to **Local Device > System Access Log**.
3. Go to the search bar.
4. Click .
The **Advanced Search** window appears.
5. Specify the following filter fields:

| Fields | Steps |
|---------------------------|---|
| Severity Level | <ol style="list-style-type: none"> a. Click . The severity level drop-down menu appears. b. Select a severity level option. |
| Accessed Resources | <ol style="list-style-type: none"> a. Click . The content condition option appears. b. Select a condition. c. Specify the keywords. |
| Date | <ol style="list-style-type: none"> a. Click . The date drop-down menu appears. b. Select a date option. |
| Connection type | <ol style="list-style-type: none"> a. Click . The connection type option appears. b. Select a connection type. |
| User | <ol style="list-style-type: none"> a. Click . The user condition option appears. b. Select a condition. c. Specify the keywords. |
| Action | <ol style="list-style-type: none"> a. Click . The action drop-down menu appears. b. Select an action option. |

| Fields | Steps |
|------------------|---|
| Source IP | <ol style="list-style-type: none"> a. Click  . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address. |

6. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.

7. Click **Search**.
The list of filtered results is displayed.

8. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.

9. Enter a tab name.

10. Click **Apply**.
- The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.



Local Log Settings



Log Settings allows you to configure the following types of settings: event logs, access logs, display styles, and event indicators.

Configuring Event Log Settings

You can specify the database size and the log language or delete all the log entries for system event logs.

1. Open QuLog Center.
2. Go to **Local Device > Log Settings > Event Log Settings** .
3. Specify the following settings:

| Settings | Steps |
|--------------------|---|
| Destination | <ol style="list-style-type: none"> a. Click  . The log destination option drop-down menu appears. b. Select a log destination. <p> Important</p> <ul style="list-style-type: none"> • You must configure a log destination to enable event logging features. • You cannot select a volume that is encrypted or has less than 10% of free volume space. |

| Settings | Steps |
|--|---|
| Maximum number of entries | <ol style="list-style-type: none"> a. Click  . The maximum number of entries option drop-down menu appears. b. Select the maximum number of entries allowed. The log database size is specified. |
| Log retention time | <ol style="list-style-type: none"> a. Click  . The log retention time drop-down menu appears. b. Select the log retention time. |
| Archive overflow log entries to a standby log destination | <ol style="list-style-type: none"> a. Click Archive and move log entries to the specified location after reaching the database limit. The destination folder option is activated. b. Click Browse. The Select a shared folder window appears. c. Select a shared folder. d. Click OK. The shared folder is selected as the standby log destination. |

4. Optional: Delete all event logs.


- a. Click **Delete All Event Logs**.
A confirmation message appears.
- b. Click **Yes**.



Warning

You cannot restore deleted logs.

5. Select the log language.


- a. Click  .
The log language drop-down menu appears.
- b. Select a language.

6. Click **Apply**.

Configuring Access Log Settings

You can specify the database size and the log language, or delete all system access log entries.

1. Open QuLog Center.
2. Go to **Local Device > Log Settings > Access Log Settings** .
3. Specify the log database size.
 - a. Go to **Maximum number of entries**.

- b. Click  .
The maximum number of entries option drop-down menu appears.
 - c. Select the maximum number of entries allowed.
4. Optional: Delete all event logs.
 - a. Click **Delete All Access Logs**.
A confirmation message appears.
 - b. Click **Yes**.



Warning

You cannot restore deleted logs.

5. Select the connection types.



Tip

You can select multiple connection types.


6. Click **Apply**.

Configuring Display Settings




You can customize your log display style to enhance readability or to highlight certain entries.

1. Open QuLog Center.
2. Open **Display Settings** through one of the following methods:

| Accessing Display Setting Method | Steps |
|----------------------------------|---|
| System Event Log | Go to Local Device > System Event Log > Display style . |
| System Access Log | Go to Local Device > System Access Log > Display style . |

3. Click  .
The display style drop-down menu appears.
4. Click **Settings**.
The **Display Style Settings** window appears.
5. Perform one or more of the following tasks:

| Task | Steps |
|---------------------|---|
| Add a display style | <ol style="list-style-type: none"> a. Click Add Style. The Add Style window appears. b. Specify a name for the style. c. Click Apply. |
| Delete a style | <ol style="list-style-type: none"> a. Select a display style. b. Click Delete Style. A confirmation message appears. c. Click Yes. |

| Task | Steps |
|-------------------------------|---|
| Add a rule to a display style | <p>a. Select a display style.</p> <p>b. Click Add Rule. The Style Rule window appears.</p> <p>c. Select a field.</p> <p>d. Select a keyword.</p> <p>e. Select one or more formatting effects.</p> <p> Tip You can instantly preview the results of the selected formatting effects.</p> <p>f. Click Apply.</p> |
| Edit a rule | <p>a. Select a display style.</p> <p>b. Select a rule from the list.</p> <p>c. Click Edit. The Style Rule window appears.</p> <p>d. Select a field.</p> <p>e. Specify the condition.</p> <p>f. Select one or more formatting effects.</p> <p> Tip You can instantly preview the results of selected formatting effects.</p> <p>g. Click Apply.</p> |
| Remove a condition | <p>a. Select a display style.</p> <p>b. Select a condition from the list.</p> <p>c. Click Delete. A confirmation message appears.</p> <p>d. Click Yes.</p> |
| Specify the priority of rules | <p>a. Select a display style.</p> <p>b. Select a rule from the list.</p> <p>c. Beside Priority, click \wedge or \vee to change its priority.</p> <p> Note The formatting results of rules with a higher priority overwrite those with a lower priority.</p> |


Removing Event Indicators

1. Open QuLog Center.

2. Go to **Local device > Log Settings > Event Indicators** .
3. Select an event flag rule.

**Tip**

Click the box in the top left column to select all event flag rules.

4. Click **Remove** or  .
The event flag rule is removed.

QuLog Service

QuLog Service allows you to centrally manage logs from multiple remote devices. You can configure a single device as a Log Receiver to manage and monitor all incoming system logs from other devices, or configure the device as a Log Sender that sends all system logs to a remote QuLog Center.

Configuring Log Sender Settings

The Log Sender allows you to send system event logs and system access logs on the local device to a remote QuLog Center or Syslog Server.

Adding a Destination IP Address

1. Open QuLog Center.
2. Select one of the following options:

| Options | User Actions |
|------------------------------|--|
| Send to QuLog Center | <ol style="list-style-type: none"> a. Go to QuLog Service > Log Sender > Send to QuLog Center . b. Enable Send logs to a remote QuLog Center. System event logs and access logs from the local device are sent to a remote QuLog Center. |
| Send to Syslog Server | <ol style="list-style-type: none"> a. Go to QuLog Service > Log Sender > Send to Syslog Server . b. Enable Send logs to a remote QuLog Center. System event logs and access logs from the local device are sent to a remote syslog server. |

3. Click **Add Destination**.
The **Add Destination** window appears.
4. Specify the following IP address information:

- **Destination IP**

**Tip**

You can enter the destination IP address manually or click **Search** to automatically select a device from your local network.

- **Port**
- **Transfer protocol**

- **Log type**
- **Format**




Note


You can click **Send a Test Message** to test the connection.

5. Click **Apply**.

Editing a Destination IP Address

1. Open QuLog Center.
2. Go to **Log Sender**.
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select a destination IP address.
5. Click  .
The **Edit Destination** window appears.
6. Edit the IP address information.
For details, see [Adding a Destination IP Address](#).
7. Click **Apply**.

Removing a Destination IP Address

1. Open QuLog Center.
2. Go to **QuLog Service > Log Sender** .
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select one or multiple destination IP addresses.
5. Click **Remove** or  .
A confirmation message window appears.
6. Click **Yes**.
The destination IP address is removed.

Configuring Log Reciever Settings

The Log Reciever allows you to configure a local device as the recipient of remote device logs. You can centrally manage and monitor system event logs and access logs from remote QNAP devices. Additionally, you can configure customized filters to search for logs efficiently.

Configuring Log Receiver General Settings






1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > General Settings** .
3. Select **Receive logs from a remote QuLog Center**.

- Select transfer protocols and then specify the port number.

**Note**

QuLog Center supports TCP and UDP protocols.

- Optional: Click **Enable Transport Layer Security (TLS)**.
- Select **System Event Log** or **System Access Log**.
- Specify the following settings:

| Settings | Steps |
|--|--|
| Destination | <ol style="list-style-type: none"> Click  . The log destination option drop-down menu appears. Select a log destination. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Important You cannot select a volume that is encrypted or has less than 10% of free volume space.</p> </div> |
| Maximum number of entries | <ol style="list-style-type: none"> Click  . The maximum number of entries option drop-down menu appears. Select the maximum number of entries allowed. The log database size is specified. |
| Log retention time | <ol style="list-style-type: none"> Click  . The log retention time drop-down menu appears. Select the log retention time. |
| Archive overflow log entries to a standby log destination | <ol style="list-style-type: none"> Click Archive and move log entries to the specified location after reaching the database limit. The destination folder option is activated. Click Browse. The Select a shared folder window appears. Select a shared folder. Click OK. The shared folder is selected as the standby log destination. |
| Delete all event logs | <ol style="list-style-type: none"> Click Delete All Event Logs. A confirmation window appears. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Warning You cannot restore deleted logs.</p> </div> <ol style="list-style-type: none"> Click Yes. |

- Click **Apply**.

Log Filter Configurations

You can specify log filter conditions for system logs received from multiple sender devices on the Log Receiver to simplify locating specific types of logs and monitoring large volume of logs.

Configuring a Log Filter Criterion

You can specify log filter criteria to choose the types of log entries that will be received by Log Receiver.

1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Select **System Event Log** or **System Access Log**.
4. Click **Add Filter Criteria**.
The filter criteria window appears.
5. Specify the following information:


| Log Type | Settings |
|--------------------------|--|
| System Event Log | <ul style="list-style-type: none"> • Severity level • User • Source IP • Application • Category • Content |
| System Access Log | <ul style="list-style-type: none"> • Severity level • User • Source IP • Connection type • Accessed resources • Action |

6. Click **Apply**.


QuLog Center adds the specified log filter criteria.

Editing a Log Filter Criterion


1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Go to **System Event Log** or **System Access Log**.
4. Select a filter criteria.
5. Optional: Click **Reset** to clear all filter criteria settings.

6. Click  .
The **Filter Criteria** window appears.
7. Edit the log filter fields.
For details, see [Configuring a Log Filter Criterion](#).
8. Click **Apply**.
All changes are applied.

Deleting a Log Filter Criterion

1. Open QuLog Center.
2. Go to **QuLog Service > QuLog Server > Filter Criteria** .
3. Select **System Event Log** or **System Access Log**.
4. Select a filter criteria.
5. Click  .
A confirmation window appears.
6. Click **Yes**.

Importing a Custom Filter Criterion

1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Click **System Event Log** or **System Access Log**.
4. Click **Add Filter Criteria**.
5. Go to **Import custom filter criteria from the selected tab**.
6. Click  .
The custom filter criteria drop-down menu appears.
7. Select the custom filter tab from the drop-down menu.



Note

For details on how to create a custom filter tab, see the following topics:

- [Creating a Custom Filter Tab for System Event Log on a Sender Device](#)
- [Creating a Custom Filter Tab for System Access Log on a Sender Device](#)

The selected custom filter criteria are applied to the log.

Viewing and Managing Remote Logs

You can view and manage remote logs under the Sender Devices section in QuLog Center. This section lists all remote devices that send their logs to the QuLog Center on the local device. You can monitor logs from all sender devices or from individual sender devices. QuLog Center can manage up to 500 sender devices on a log receiver.

Managing System Event Logs on the Log Receiver

You can monitor and manage system event logs received by the **Log Receiver** in **QuLog Service > All Devices > System Event Log** . You can also monitor system event logs from individual sender devices.











Important

You must configure the log destination of the log receiver to enable this feature. For details, see [Configuring Log Receiver General Settings](#).

On the **System Event Log** screen, you can perform the following tasks:

| Task | Steps |
|-----------------------------------|--|
| Select a group mode | <ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By app: this mode groups log entries by app name. • By date: this mode groups log entries by date. • By content: this mode groups log entries by log content. • By user: this mode groups log entries by users. • By source IP: this mode groups log entries by source IP address. • By Host Name: this mode groups log entries by the host name. |
| Select a display style | <ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click Add Style to create a display style. For details, see Configuring Display Settings.</p> |
| Create an event notification rule | <p>You can quickly create an event notification rule using a log entry. This allows you to receive notifications for events similar to the selected log entry.</p> <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event notification rule. Notification Center opens and the Create event notification rule windows appears. For details, see Creating an Event Notification Rule. |

| Task | Steps |
|---------------------------|--|
| Create an event flag rule | <p>You can quickly create an event flag rule using a log entry. This allows you to set event indicators for malware detection.</p> <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event flag rule. The Create Event Flag Rule window appears. 4. Click Create. The log flag rule is created. |
| Export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 7. Click Export. |
| Download export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer. |

| Task | Steps |
|--------------------------------|---|
| Perform a search | <ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. <p>For details, see Creating a Custom Filter Tab for System Event Log on the Sender Device.</p> |
| Select display items | <ol style="list-style-type: none"> 1. Click . 2. Select the items to display. |
| Select all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all. |
| Deselect all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection. |
| Copy one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere. |
| Delete one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes. |

Managing System Access Logs on the Log Receiver








You can monitor and manage system access logs received by the **Log Receiver** in **QuLog Service > All Devices > System Access Log**. You can also monitor system access logs from individual sender devices by clicking on the device.






Important

You must configure the log destination of the log receiver to enable this feature.
For details, see [Configuring Log Receiver General Settings](#).

On the **System Access Log** tab, you can perform the following tasks:

| Task | Steps |
|------------------------|---|
| Select a group mode | <ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By date: this mode groups log entries by date. • By user: this mode groups log entries by user. • By source IP: this mode groups log entries by source IP. • By Host Name: this mode groups log entries by host name. |
| Select a display style | <ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click  and select Create a Style to create a display style. For details, see Configuring Display Settings.</p> |
| Export logs | <ol style="list-style-type: none"> 1. Click . The Export Logs window appears. 2. Select an export file format. 3. Specify the maximum number of log entries per file. 4. Optional: Compress the export file and specify a password. 5. Click Export. |
| Download exported logs | <ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer. |

| Task | Steps |
|--------------------------------|---|
| Perform a search | <ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for System Access Log on the Sender Device. |
| Select display items | <ol style="list-style-type: none"> 1. Click . 2. Select the items to display. |
| Select all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all. |
| Deselect all log entries | <ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection. |
| Copy one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere. |
| Delete one or more log entries | <ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes. |


Logging in a Sender Device






1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Select a device.
4. Click **Settings**.
5. Specify the following:
 - **Host IP address**
 - **Port**
 - **Username**
 - **Password**
6. Optional: Select **Secure login (HTTPS)**.

7. Click **Sign in**.

- You are logged into the sender device.
- All destination IP addresses of the sender device are listed.
- You can configure the destination for sender device logs.
For details, see [Configuring Log Sender Settings](#).

Creating a Custom Filter Tab for System Event Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Click on a sender device.
4. Go to **System Event Log** .
5. Go to the search bar.
6. Click  .
7. Specify the following filter fields:

| Fields | Steps |
|-----------------------|--|
| Severity Level | <ol style="list-style-type: none"> Click  . The severity level drop-down menu appears. Select a severity level option. |
| Application | <ol style="list-style-type: none"> Click  . The application drop-down menu appears. Select an application. The Category option appears. <p> Note The Category option does not appear if you select any applications or do not specify the application.</p> <ol style="list-style-type: none"> Specify the application Category. |
| Date | <ol style="list-style-type: none"> Click  . The date drop-down menu appears. Select a date option. |
| Content | <ol style="list-style-type: none"> Click  . The content condition option appears. Select a condition. Specify the content keywords. |

| Fields | Steps |
|------------------|---|
| User | <ol style="list-style-type: none"> a. Click ▾ . The user condition option appears. b. Select a condition. c. Specify the keywords. |
| Source IP | <ol style="list-style-type: none"> a. Click ▾ . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address. |

8. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
9. Click **Search**.
The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.
11. Enter a tab name.
12. Click **Apply**.
 - The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.

Creating a Custom Filter Tab for System Access Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Click on a sender device.
4. Go to **System Access Log** .
5. Go to the search bar.
6. Click ▾ .
7. Specify the following filter fields:

| Fields | Steps |
|-----------------------|---|
| Severity Level | <ol style="list-style-type: none"> a. Click ▾ . The severity level drop-down menu appears. b. Select a severity level option. |

| Fields | Steps |
|---------------------------|---|
| Accessed Resources | <ol style="list-style-type: none"> a. Click ▾ . The content condition option appears. b. Select a condition. c. Specify the keywords. |
| Date | <ol style="list-style-type: none"> a. Click ▾ . The date drop-down menu appears. b. Select a date option. |
| Connection type | <ol style="list-style-type: none"> a. Click ▾ . The connection type option appears. b. Select a connection type. |
| User | <ol style="list-style-type: none"> a. Click ▾ . The user condition option appears. b. Select a condition. c. Specify the keywords. |
| Action | <ol style="list-style-type: none"> a. Click ▾ . The action drop-down menu appears. b. Select an action option. |
| Source IP | <ol style="list-style-type: none"> a. Click ▾ . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address. |

8. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.

9. Click **Search**.
The list of filtered results is displayed.

10. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.


11. Enter a tab name.

12. Click **Apply**.

- The custom filter tab is created.
- The custom filter tab is displayed next to the **Main** tab.

Configuring Event Indicators on the Sender Device

The event severity indicators on the device list are displayed according to the event severity level (information, warning, and error) that occurs over a specified period. Only the highest severity level icon is displayed when multiple events occur.

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Select a device.
4. Click **Event Indicators**.
5. Click  .
The event period drop-down menu appears.
6. Select the event period.
Events that meet the specified criteria are listed in the Event Flag Rules table below.

**Tip**

You can remove event flag rules from the list.



Notification Settings


You can configure notification rules in Notification Center. You can also create filters for sending local NAS system access logs, QuLog Service system event logs, and QuLog Service system access logs.

Configuring Notification Rule Settings

QuLog Center can send notifications to recipients when the **Log Receiver** receives system event logs or system access logs from the **Log Sender**.

1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select the log types.
4. You can perform any of the following actions:

| Setting | Steps |
|----------------------------|--|
| Create a notification rule | <p>a. Click Configure Notification Rule. Notification Center opens. Follow the instructions on the Create event notification rule wizard to add an event notification rule for QuLog Center. For details, see Creating an Event Notification Rule.</p> <p> Important You must select the Log filter criteria option in System Notification Rules when creating QuLog Center notification rules for receiving local device logs, QuLog Service system event logs, and QuLog Service system access logs. To enable the Log filter criteria option, go to Notification Center > System Notification Rules > QuLog Center > Log Filter Criteria .</p> <p>b. Click Apply. The notification rule is created.</p> |
| Edit a notification rule | Click  . |

| Setting | Steps |
|---------------------------------------|--|
| Enable or disable a notification rule | Click toggle. |
| Delete a notification rule | <ol style="list-style-type: none"> a. Click . A confirmation message window appears. b. Click Yes. The notification rule is deleted. |
| View notification history | Click View notification history . Notification Center opens and displays the QuLog Center notification history page. |

Adding a Log Filter


You can add filter criteria to local NAS system access logs, QuLog Service system event logs, and QuLog Service system access logs. The filtered log results are sent to Notification Center.

1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select a system log type.
4. Click **Add Filter Criteria**.
The filter criteria window appears.
5. Specify the following information:


| Log Type | Settings |
|--------------------------|--|
| System Event Log | <ul style="list-style-type: none"> • Severity level • User • Source IP • Application • Category • Content |
| System Access Log | <ul style="list-style-type: none"> • Severity level • User • Source IP • Connection type • Accessed resources • Action |

6. Click **Apply**.
The filter is applied to logs sent to Notification Center.

Editing a Log Filter

1. Open QuLog Center.
2. Go to **QuLog Service > Notification Settings** .
3. Select a filter criteria.
4. Optional: Click **Reset** to clear all filter criteria settings.
5. Click  .
The **Filter Criteria** window appears.
6. Edit the log filter criteria.
For details, see [Adding a Log Filter](#).
7. Click **Apply**.
All changes are applied.

Removing a Log Filter

1. Open QuLog Center.
2. Go to **QuLog Service > Notification Settings** .
3. Select a filter criteria.
4. Click  .
A confirmation message window appears.
5. Click **Yes**.
The filter criteria is removed.

17. Notification Center

Notification Center consolidates all QTS notifications to help you monitor the status of your NAS and its applications and address potential issues more closely and promptly. You can send notifications to recipients through different channels including emails, SMS, instant messaging, and other push services. Notification Center also lets you create custom notification rules and criteria, ensuring that you receive notifications that are most relevant to your needs.

Overview

The **Overview** screen displays the number of notifications delivered over a specific period of time. It also displays the number of notification rules, service accounts, and paired devices you configured.

In Overview, you can view the number of messages sent over a specific period of time. You can also view the settings of notification rules, service accounts, and device pairing.

System Notification Rules More **Service Account and Device Pairing** More

| Event Notifications | Alert Notifications | E-mail | SMS | Instant Messaging | Push Service |
|---------------------|---------------------|--------|----------|-------------------|--------------|
| Inactive | Inactive | Active | Inactive | Inactive | Inactive |

System Logs Last 50 Logs last 30 days: Warning:1515 Error:53601 | More

| Seve... | Date and Time | Users | Source IP | Application | Category | Content | Action |
|---------------------------------------|---------------------|---------|-----------|---------------------|----------------------|--|--|
| i | 2020/07/08 15:34:38 | System | 127.0.0.1 | myQNAPcloud | My DDNS | [myQNAPcloud] DDNS updated WAN IP address to "218.210.98.62". | Settings |
| ! | 2020/07/08 15:00:01 | System | 127.0.0.1 | Storage & Snapshots | LUN Import/Export | [Storage & Snapshots] Failed to start LUN import/export job "LUN_Export100GB_Export1". The job is invalid. | Settings |
| i | 2020/07/08 14:56:35 | Qcenter | 127.0.0.1 | Q'center Agent | Q'center Information | [Q'center Agent] The connection between the NAS and Q'center has returned to normal. NAS name: TW-TEST1, Q'center server: 127.0.0.1. | Settings |
| i | 2020/07/08 14:54:39 | System | 127.0.0.1 | myQNAPcloud | My DDNS | [myQNAPcloud] DDNS updated WAN IP address to "60.248.95.192". | Settings |
| i | 2020/07/08 14:24:38 | System | 127.0.0.1 | myQNAPcloud | My DDNS | [myQNAPcloud] DDNS updated WAN IP address to "218.210.98.62". | Settings |
| ! | 2020/07/08 14:00:00 | System | 127.0.0.1 | Storage & Snapshots | LUN Import/Export | [Storage & Snapshots] Failed to start LUN import/export job "LUN_Export100GB_Export1". The job is invalid. | Settings |

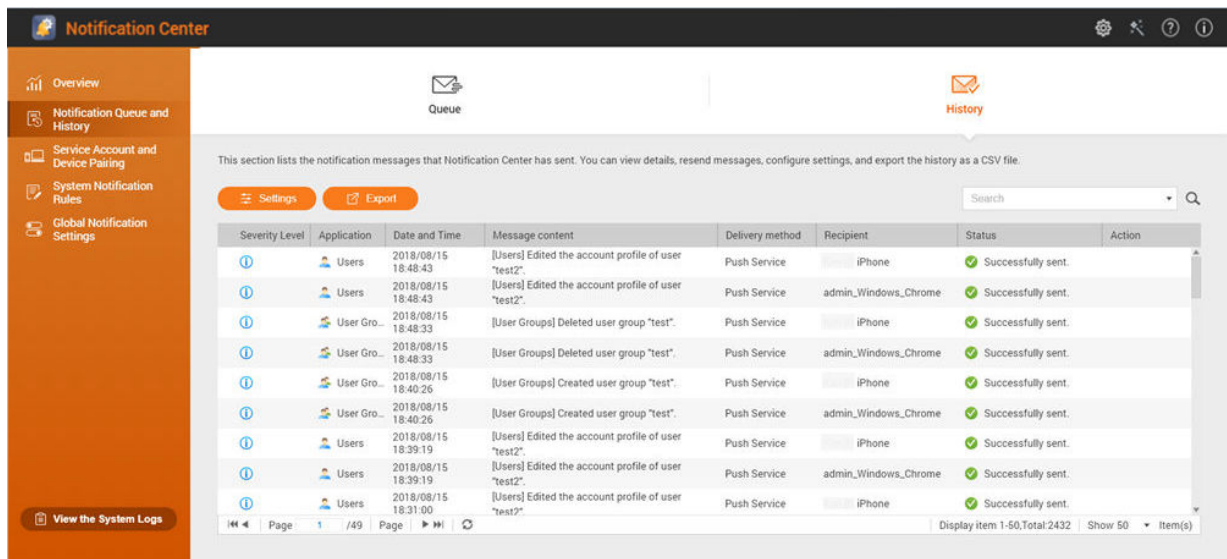
Notification Queue and History


Queue

The **Queue** screen displays the messages that Notification Center is going to send. The required transmission time depends on the current status of your NAS. You can remove a message from the queue before it is sent. Messages removed from the queue will not appear in the **History** screen.

History

The **History** screen displays the messages that Notification Center has sent. You can view details, resend messages, configure settings, and export the history as a CSV file. In the settings, you can specify how long your notification records are retained and where they are stored.



| No. | Task | User Action |
|-----|--|--|
| 1 | Export the notification message history. | Click Export . Notification Center saves the CSV file on your computer. |
| 2 | Resend the notification. | Identify the notification you want to resend, and then click  . This button only appears when Notification Center is unable to send the notification to the recipient. |

Configuring History Settings

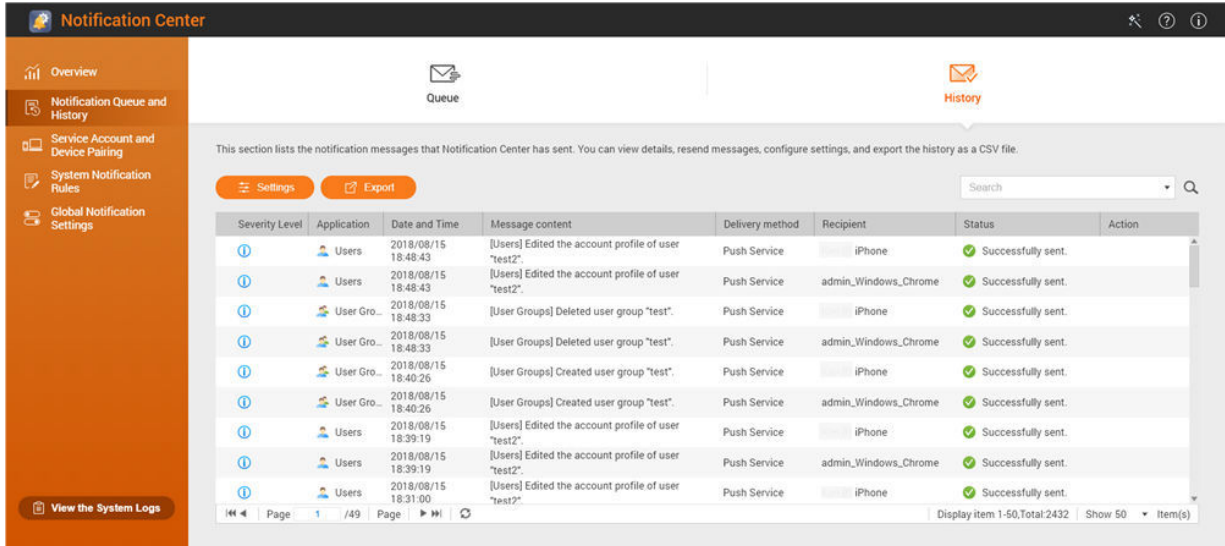
1. Open Notification Center.
2. Go to **Notification Queue and History > History** .
3. Click **Settings**.
The **Settings** window appears.
4. Configure the following information.
 - Retention period: Specify the maximum number of days Notification Center retains notification records before deleting them.
 - Notification record storage: Select whether or not you want to keep notification records in a specified local folder.
5. Click **Confirm**.
Notification Center saves your settings.







Service Account and Device Pairing

Service Account and Device Pairing allows you to configure the simple mail transfer protocol (SMTP) and short message service center (SMSC) settings so you can receive notifications through email and SMS. You can also pair your instant messaging accounts and devices with your NAS to receive notifications through instant messaging or push services.

Email Notifications


The **Email** screen allows you to add and view email notification recipients and configure your simple mail transfer protocol (SMTP) service settings.



| Button | Task | User Action |
|---|--|---|
|  | Send a test message to a specified recipient. | <ol style="list-style-type: none"> 1. Click . The Send test message window appears. 2. Specify an email address. 3. Click Send. |
|  | Edit the configurations of an existing email server. | <ol style="list-style-type: none"> 1. Click . The Edit SMTP Service Account window appears. 2. Edit the settings. 3. Click Confirm. |
|  | Remove an email server. | <ol style="list-style-type: none"> 1. Click . A confirmation message appears. 2. Click Confirm. |


Configuring an Email Notification Server

1. Go to **Service Account and Device Pairing > E-mail** .
2. Click **Add SMTP Service**.
The **Add SMTP Service** window appears.
3. Select an email account.
4. Configure the following.

| Service Providers | User Actions |
|-------------------|---|
| Outlook | <ol style="list-style-type: none"> a. Click Add account. The email account window appears. b. Specify the email address that will act as the sender for QTS notifications. A confirmation message appears. c. Click Allow. |
| Gmail | <ol style="list-style-type: none"> a. Click Add account. The email account window appears. b. Specify the email address that will act as the sender for QTS notifications. A warning notification appears. c. Click Advanced. d. Click Go to connector alpha-myqnapcloud.com (unsafe). e. Click Allow. |
| Yahoo | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Important Before configuring the Yahoo Mail settings, do the following.</p> <ol style="list-style-type: none"> a. Log in to your Yahoo Mail account. b. Go to Help > Account Info > Account Security . c. Enable Allow apps that use less secure sign in. </div> </div> <p>Return to Notification Center and specify a valid Yahoo mail address and password.</p> |
| Custom | <ol style="list-style-type: none"> a. Specify the domain name or the IP address of your SMTP service such as <code>smtp.gmail.com</code>. b. Specify the port number for the SMTP server. If you specified an SMTP port when you configured the port forwarding settings, use this port number. c. Specify the email address that will act as the sender for QTS notifications. d. Specify a username that contains a maximum of 128 ASCII characters. e. Specify a password that contains a maximum of 128 ASCII characters. f. Select one of the following secure connection options. <ul style="list-style-type: none"> • SSL: Use SSL to secure the connection. • TLS: Use TLS to secure the connection. • None: Do not use a secure connection. <p>QNAP recommends enabling a secure connection if the SMTP server supports it.</p> |
| Others | Specify a valid email address and its account password. |

**Tip**

To configure multiple email servers, click **Add SMTP Service**, and then perform the previous steps.

5. Optional: Select **Set as default SMTP service account**.
6. Optional: Click .
The SMTP server sends a test email.
7. Click **Create**.
Notification Center adds the SMTP service to the list.
8. Optional: Click **Re-configuration**.




Note

Click **Re-configuration** if you want to immediately reset the email notification server. You must repeat steps 1 to 7 for re-configuration.

Pairing Notification Center with a Web Browser

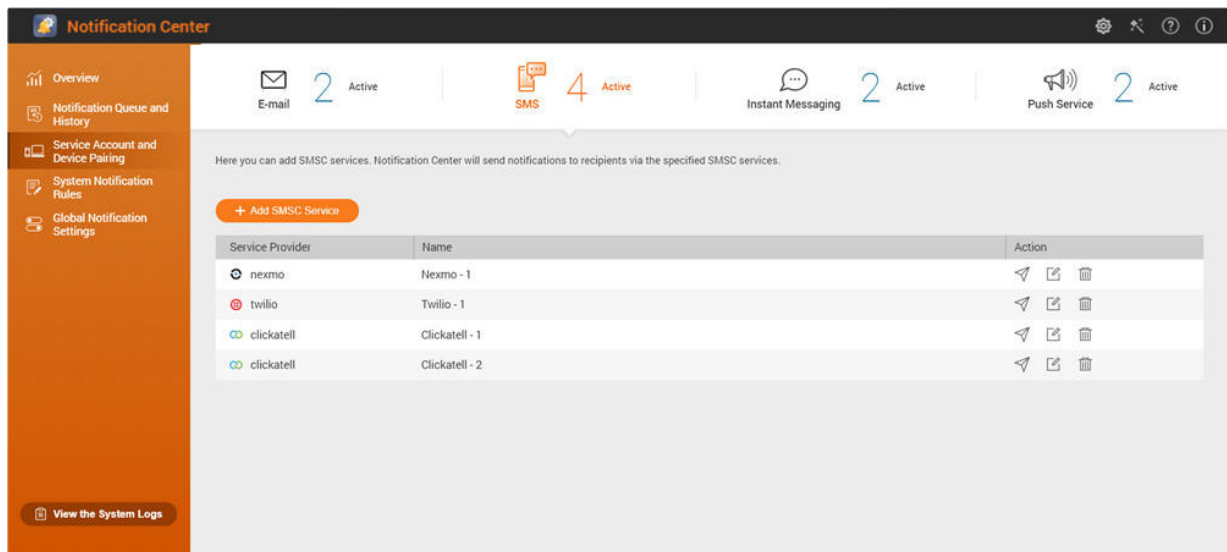
Before pairing, ensure the following.







- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers: Google Chrome, Firefox, or Safari.

1. Go to **Service Account and Device Pairing > Push Service**.
2. Under Browser, click **Pair**.
Notification Center pairs with your current browser.
The browser appears in the list of paired devices.
3. Change your browser name.
 - a. Beside your browser name, click .
 - b. Specify a browser name.
The field accepts a maximum of 127 ASCII characters.
 - c. Press ENTER.
Notification Center saves your browser name.

SMS Notifications


The SMS screen allows you to view and configure your short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Nexmo, and Twilio.



| Button | Task | User Action |
|---|--|---|
|  | Send a test message to a specified recipient. | <ol style="list-style-type: none"> 1. Click . The Send test message window appears. 2. Specify a country code and phone number. 3. Click Send. |
|  | Edit the configurations of an existing SMS server. | <ol style="list-style-type: none"> 1. Click . The Edit SMSC Service Account window appears. 2. Edit the settings. 3. Click Confirm. |
|  | Remove an SMS server. | <ol style="list-style-type: none"> 1. Click . A confirmation message appears. 2. Click Confirm. |

Configuring an SMS Notification

1. Go to **Service Account and Device Pairing > SMS** .
2. Click **Add SMSC Service**.
The **Add SMSC Service** window appears.
3. Select a service provider.
4. Specify an alias.
5. Specify the following information.

| SMS Service Provider | Information |
|-----------------------------------|---|
| Clickatell - Communicator/Central | Clickatell username, password, and API ID |
| Clickatell - SMS Platform | Clickatell API key |
| Nexmo | Nexmo API key and secret question, and a sender name The sender name can contain a maximum of 32 characters. |
| Twilio | Your Twilio account SID, access token, and the Twilio-provided phone number linked to your account |
| Custom | <ul style="list-style-type: none"> URL template text formatted according to the format specified by your SMS service provider. Use the following replaceable URL template parameters. <ul style="list-style-type: none"> @@UserName@@: Specify the username for this connection. @@Password@@: Specify the password for this connection. @@PhoneNumber@@: Specify the phone number where the SMS messages are sent. This parameter is required. @@Text@@: Specify the text content of the SMS message. This parameter is required. <p> Important You will not be able to receive SMS messages if the template text does not match the format used by your SMS service provider.</p> <ul style="list-style-type: none"> The name of the service provider. The name can contain a maximum of 32 ASCII characters. A password. The password can contain a maximum of 32 ASCII characters. |



Tip

To configure multiple SMS servers, click **Add SMSC Service**, and then perform the previous steps.

6.

Click .

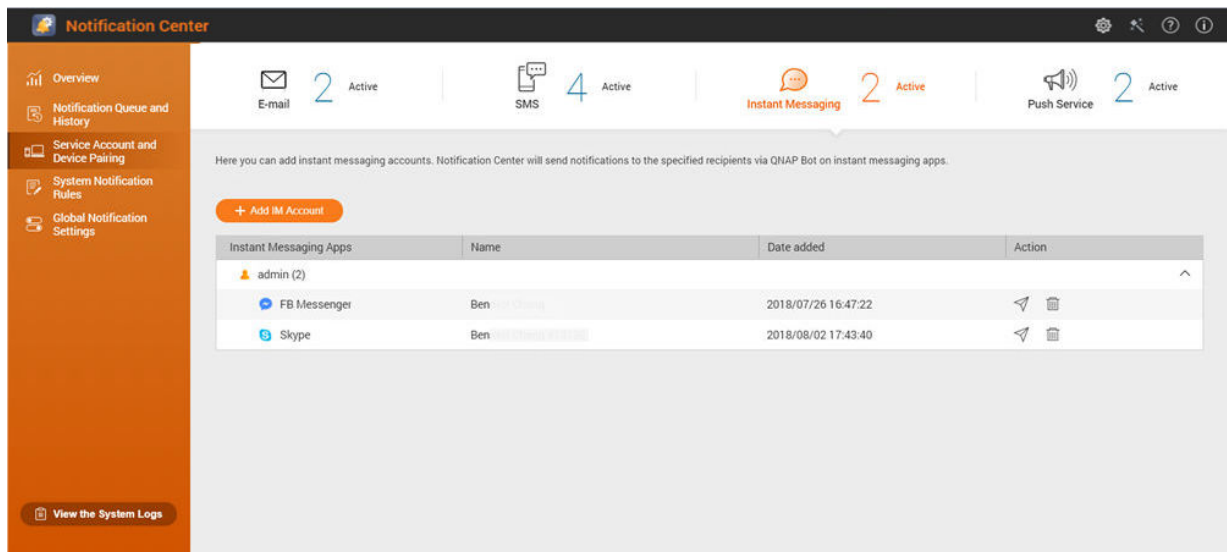
The SMS server sends a test message.





7. Click **Create**.

Notification Center adds the SMTP service to the list.

Instant Messaging Notifications

The Instant Messaging screen allows you to pair Notification Center with instant messaging accounts such as Skype and Facebook Messenger. Notification Center sends notifications to the specified recipients through QBot, the QNAP instant messaging bot account.



| Button | Task | User Action |
|--|---|---|
|  | Send a test message. | Click  . |
|  | Unpair from and remove the instant messaging account. | <ol style="list-style-type: none"> Click . A confirmation message appears. Click Confirm. |

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Skype account.
- Skype is installed on your device.

1. Go to **Service Account and Device Pairing > Instant Messaging**.
2. Click **Add IM Account**.
The **Notification IM Wizard** appears.
3. Select Skype.
The **Add Bot to Contacts** window appears.
4. Log in to the Skype account you want to pair.
Skype adds QNAP Bot as a contact.
5. Close the **Add Bot to Contacts** window.
6. Click **Next**.
A verification code appears.
7. On Skype, enter the verification code.
Notification Center verifies and pairs with the Skype account.

- Click **Finish**.
Notification Center adds the Skype account to the list.

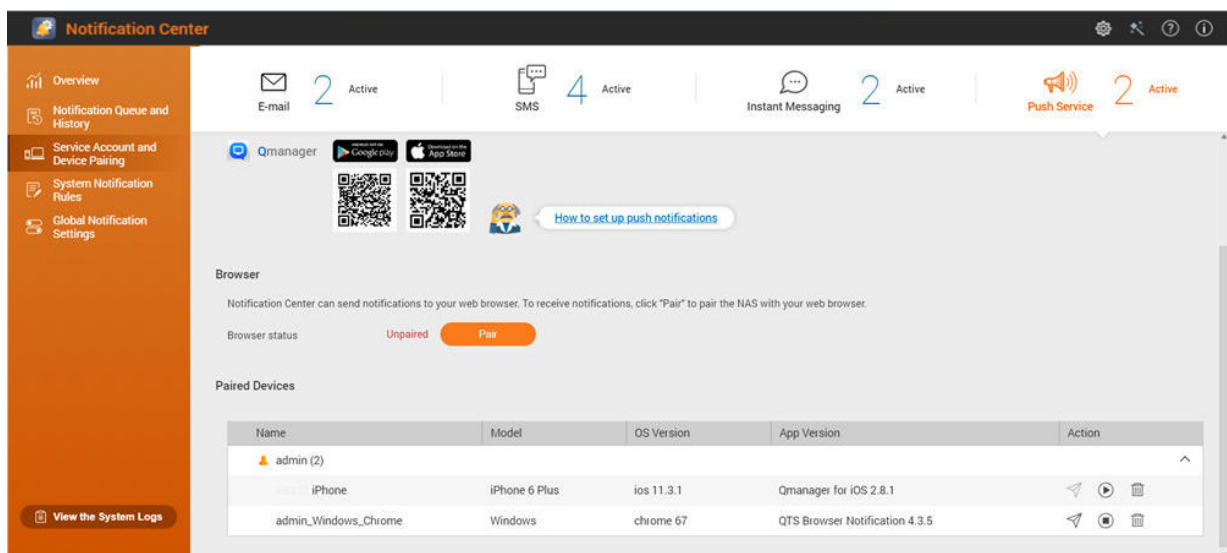
Pairing Notification Center with Facebook Messenger









Before configuring instant messaging (IM) notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
 - You have an active Facebook Messenger account.
- Go to **Service Account and Device Pairing > Instant Messaging**.
 - Click **Add IM Account**.
The **Notification IM Wizard** appears.
 - Select Facebook Messenger.
The **Add Bot to Contacts** window appears.
 - Log in to the Facebook Messenger account you want to pair.
Facebook Messenger adds QNAP Bot as a contact.
 - Click **Get Started**.
A verification code appears on the **Notification IM Wizard**.
 - On Facebook Messenger, enter the verification code.
Notification Center verifies and pairs with the Facebook Messenger account.
 - Click **Finish**.
Notification Center adds the Facebook Messenger account to the list.

Push Notifications

The Push Service screen allows you to configure push services for web browsers and mobile devices.




| Button | Task | User Action |
|---|--|---|
|  | Send a test message. | Click  . |
|  | Start sending push notifications to the device or browser. | Click  . |
|  | Stop sending push notifications to the device or browser. | Click  . |
|  | Unpair and remove the device or browser. | <ol style="list-style-type: none"> Click . A confirmation message appears. Click Confirm. |

Pairing Notification Center with a Mobile Device

Before pairing, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- Qmanager is installed on the mobile device.
- Your NAS is added in Qmanager.

1. Open Qmanager on the mobile device.
2. Perform one of the following.

| Pairing Option | User Action |
|-------------------|---|
| Automatic pairing | <ol style="list-style-type: none"> a. From the device list, click the NAS you want to pair. A confirmation message appears. b. Click Confirm. |
| Manual pairing | <ol style="list-style-type: none"> a. Identify your NAS from the device list, and then click . The device settings screen appears. b. Select Push notifications. c. Click Save. A confirmation message appears. d. Click Confirm. |


Notification Center pairs with the mobile device.

3. In Notification Center, go to **Service Account and Device Pairing > Push Service**.
4. Verify that the mobile device appears in the list of paired devices.

Pairing Notification Center with a Web Browser

Before pairing, ensure the following.

- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers: Google Chrome, Firefox, or Safari.

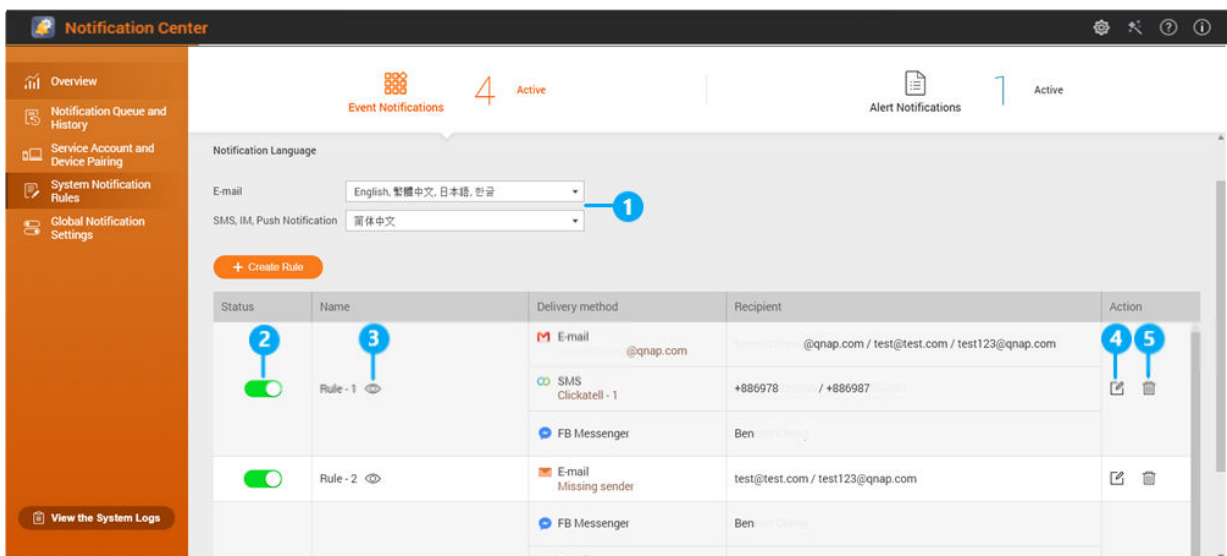
1. Go to **Service Account and Device Pairing > Push Service** .
2. Under Browser, click **Pair**.
Notification Center pairs with your current browser.
The browser appears in the list of paired devices.
3. Change your browser name.
 - a. Beside your browser name, click  .
 - b. Specify a browser name.
The field accepts a maximum of 127 ASCII characters.
 - c. Press ENTER.
Notification Center saves your browser name.


System Notification Rules




You can create and manage event notification rules to receive event notifications promptly.

Managing Event Notification Rules

You can create custom rules and select applications and features that you want to receive event notifications from. You can also specify the message type, keywords, and time range to further define notification types or narrow the scope. Notification Center supports sending event notifications in multiple languages and provides four delivery methods to meet your different needs, including emails, SMS, instant messaging, and push services.



| No. | Tasks | User Actions |
|-----|----------------------------------|---|
| 1 | Specify a notification language. | <ol style="list-style-type: none"> 1. Select one or more languages for email notifications. 2. Select a language for SMS, IM, and push notifications. |
| 2 | Enable or disable the rule. | Click  . |

| No. | Tasks | User Actions |
|-----|----------------------------|---|
| 3 | Preview the rule settings. | <ol style="list-style-type: none"> 1. Click . The Event Notifications window appears. 2. Review the settings, and then click Close. |
| 4 | Edit the rule. | <ol style="list-style-type: none"> 1. Click . The Edit Rule for Event Notifications window appears. 2. Edit the settings. 3. Click Confirm. |
| 5 | Delete the rule. | <ol style="list-style-type: none"> 1. Click . A confirmation message appears. 2. Click Confirm. |

Creating an Event Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. Go to **System Notification Rules > Event Notifications**.
2. Click **Create Rule**.
The **Create event notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.



Tip

To select all events, select **Select all**.



To display only the events for a specific application or service, select the item from the **Displayed Items** drop-down menu.

5. Click **Next**.
6. Select a severity level.

| Severity Level | Description |
|----------------|---|
| Information | Information messages inform users of changes in the NAS settings or its applications. |
| Warning | Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally. |
| Error | Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features. |

7. Specify a keyword filter.

| Filter | Description |
|--------------|---|
| All messages | Notification Center sends all notifications that are classified under the types you selected. |



| Filter | Description |
|----------|--|
| Includes | Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords. |
| Excludes | Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords. |









Important

The event notification filter only accepts keywords that are in English or in any of the languages specified on the **Event Notifications** screen.

8. Specify a time range when you want to receive notifications.
9. Click **Next**.
10. Select a delivery method.
11. Configure the sender information.

| Method | User Action |
|-----------------------------------|---|
| Email | <p>a. Select an SMTP server.</p> <p> Tip To add an SMTP server, see Configuring an Email Notification Server.</p> <p>b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive.</p> <p>c. Optional: Select Send email as plain text.</p> |
| SMS | <p>Select an SMSC server.</p> <p> Note To add an SMSC server, see Configuring an SMS Notification Server.</p> |
| Instant Messaging or Push Service | Notification Center automatically assigns Qbot. |

12. Configure the recipient information.

| Method | User Action |
|-------------------|--|
| Email | <p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click . |
| SMS | <p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p>d. Select a country code for each recipient.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click . |
| Instant Messaging | <p>Select one or more recipients.</p> <p> Tip</p> <p>To add instant messaging notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger |
| Push Service | <p>Select one or more recipients.</p> <p> Tip</p> <p>To add push notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser |

13. Optional: Click  to send a test message.

14. Optional: Click **Add Pair** to create a new pair.

15. Click **Next**.

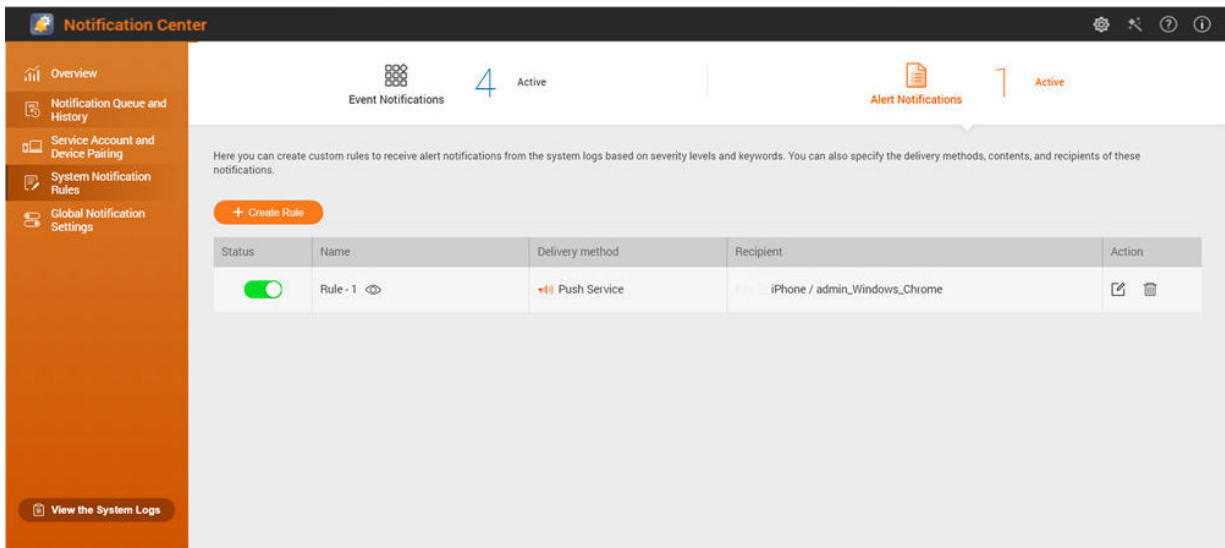
16. Verify the rule settings.

17. Click Finish.

Notification Center displays the new rule on the **Event Notifications** screen.

Alert Notifications

You can create custom rules to receive alert notifications from the System Logs based on the notification type and keywords. You can also specify the delivery methods, contents, and recipients of these notifications.



| Button | Task | User Action |
|--------|---|---|
| | Enable or disable the rule. | Click . |
| | Preview the rule settings. | <ol style="list-style-type: none"> Click . The Alert Notifications window appears. Review the settings, and then click Close. |
| | Edit the rule. | <ol style="list-style-type: none"> Click . The Edit Rule for Alert Notifications window appears. Edit the settings. Click Confirm. |
| | Unpair from and remove the device or browser. | <ol style="list-style-type: none"> Click . A confirmation message appears. Click Confirm. |

Creating an Alert Notification Rule



Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

- Go to **System Notification Rules > Alert Notifications** .

2. Click **Create Rule**.
The **Create alert notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.
 - a. Select a severity level.

| Severity Level | Description |
|----------------|---|
| Information | Information messages inform users of changes in the NAS settings or its applications. |
| Warning | Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally. |
| Error | Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features. |

- b. Optional: Specify a keyword filter.



| Filter | Description |
|--------------|--|
| All messages | Notification Center sends all notifications that are classified under the types you selected. |
| Includes | Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords. |
| Excludes | Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords. |







Important



The alert notification filter only accepts keywords that are in English.


5. Optional: Specify a time range when you want to receive notifications.
6. Optional: Specify a notification message threshold.
7. Click **Next**.
8. Select a delivery method.
9. Configure the sender information.

| Method | User Action |
|-----------------------------------|--|
| Email | <p>a. Select an SMTP server.</p> <p> Tip To add an SMTP server, see Configuring an Email Notification Server.</p> <p>b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive.</p> <p>c. Optional: Select Send email as plain text.</p> |
| SMS | <p>Select an SMSC server.</p> <p> Note To add an SMSC server, see Configuring an SMS Notification Server.</p> |
| Instant Messaging or Push Service | Notification Center automatically assigns Qbot. |


10. Configure the recipient information.

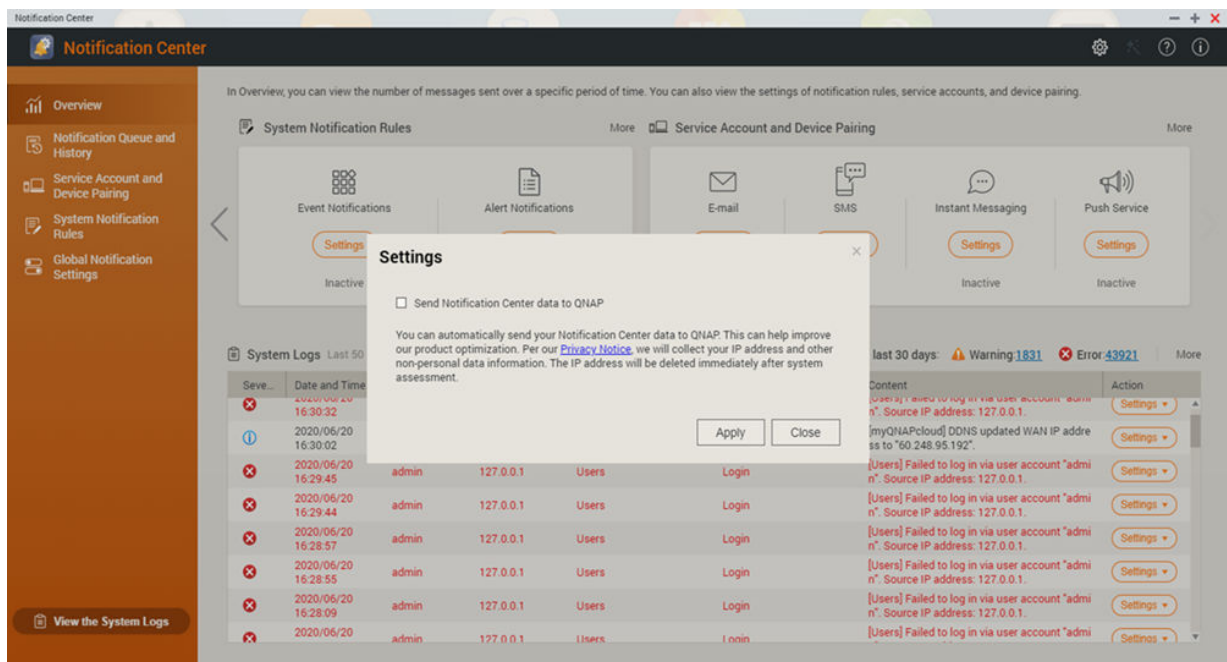
| Method | User Action |
|--------|--|
| Email | <p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click . |
| SMS | <p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p>d. Select a country code for each recipient.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click . |

| Method | User Action |
|-------------------|---|
| Instant Messaging | <p>Select one or more recipients.</p> <p> Tip To add instant messaging notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger |
| Push Service | <p>Select one or more recipients.</p> <p> Tip To add push notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser |

11. Optional: Click  to send a test message.
12. Optional: Click **Add Pair** to create a new pair.
13. Click **Next**.
14. Verify the rule settings.
15. Click **Finish**.
Notification Center displays the new rule on the **Alert Notifications** screen.

Settings

The **Settings** screen allows you to enable or disable submitting Notification Center data to QNAP. Click  to open the **Settings** window.




Enabling Send Notification Data to QNAP



Important

QNAP does not collect your personal data or information.


1. Open **Notification Center**.
2. Click .
The **Send Notification data to QNAP** window appears.
3. Select **Send Notification data to QNAP**.
4. Click **Apply**.

Disabling Send Notification Data to QNAP



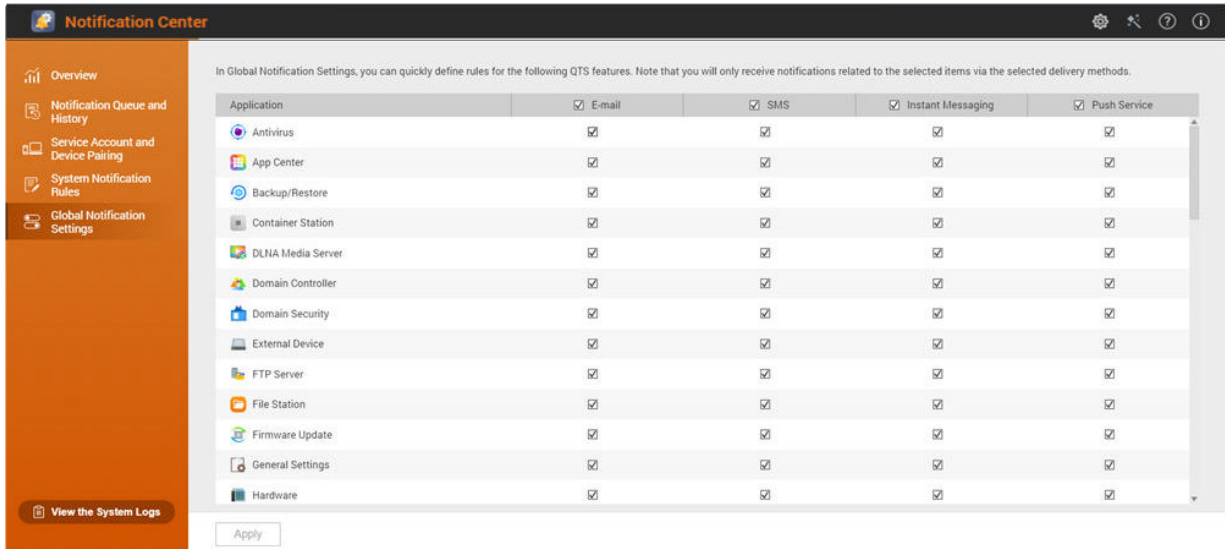
Important

QNAP does not collect your personal data or information.

1. Open **Notification Center**.
2. Click .
The **Send Notification data to QNAP** window appears.
3. Deselect **Send Notification data to QNAP**.
4. Click **Apply**,

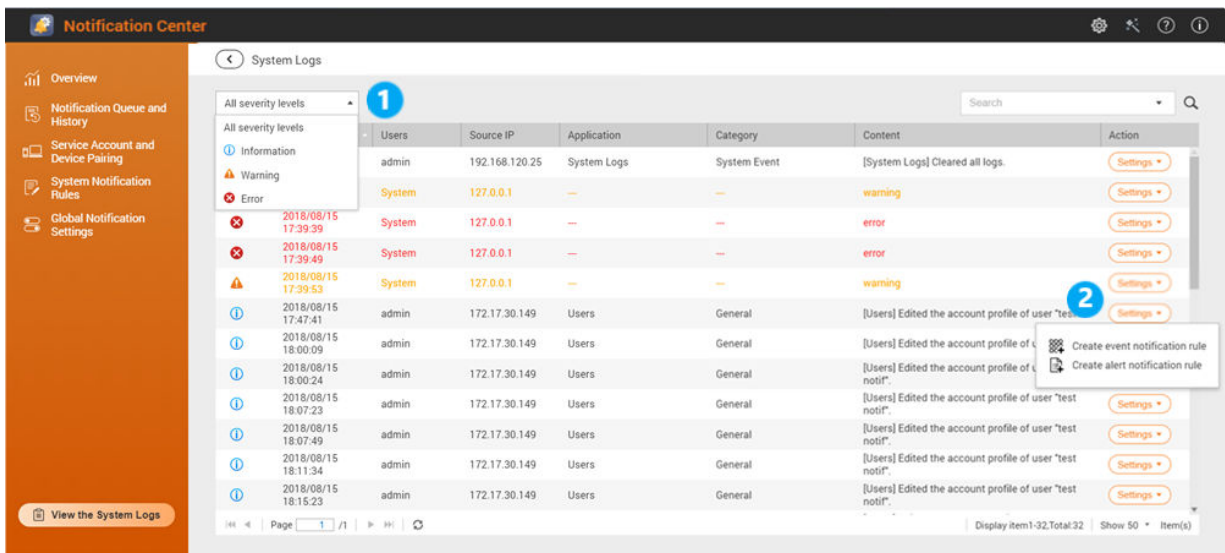
Global Notification Settings

The Global Notification Settings screen allows you to quickly define global notification rules. From the list, you can select or deselect, and then apply the delivery methods for each QTS feature or application. Users only receive notifications related to the selected features through their selected delivery methods.





System Logs

The **System Logs** screen displays all system events on the NAS. On this screen, you can sort and filter the logs or create notification rules based on existing logs.



| No. | Task | User Action |
|-----|--------------------|--------------------------|
| 1 | Filter system logs | Select a severity level. |

| No. | Task | User Action |
|-----|----------------------------|--|
| 2 | Search system logs | <p>Search for logs by keywords or through advanced search. To use advanced search follow the instructions below:</p> <ol style="list-style-type: none"> 1. Click  in the search bar. The advanced search option drop down menu appears. 2. Specify the following parameters where applicable: <ul style="list-style-type: none"> • Keyword • Severity Level • Date • Users • Source IP • Application • Category 3. Click Search. Lists all log entries that meet the specified conditions. |
| 3 | Create a notification rule | <ol style="list-style-type: none"> 1. Click Settings. 2. Select one of the following options. <ul style="list-style-type: none"> • Create event notification rule • Create alert notification rule <p>The Create notification rule window appears.</p> 3. Select one of the following options. <ul style="list-style-type: none"> • Add as a new rule • Add to an existing rule 4. Click Confirm. <p> Tip To add or edit notification rules, see the following topics:</p> <ul style="list-style-type: none"> • Creating an Event Notification Rule • Creating an Alert Notification Rule |

18. Malware Remover

About Malware Remover

Malware Remover is a built-in utility designed to protect QNAP devices against harmful software. Malware programs are often disguised as or embedded in nonmalicious files and software. They often attempt to gain access to sensitive user information and may negatively impact device performance.

Implementing several layers of protection, Malware Remover allows you to perform instant and scheduled scans on your QNAP device and prevents malicious software from putting your data at risk.

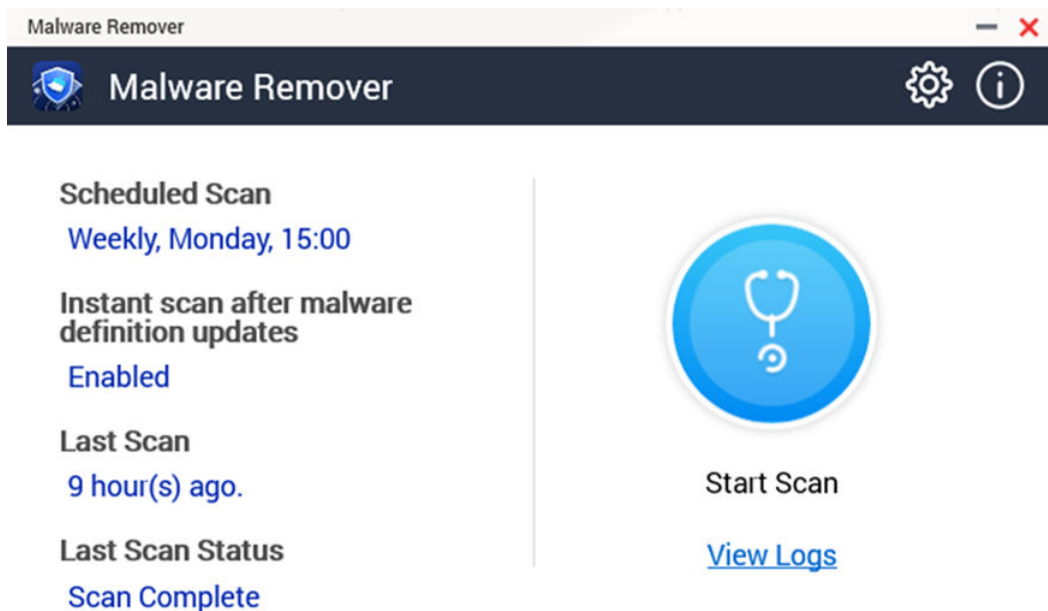


Important

QNAP strongly recommends running routine scans to prevent malware infections and protect the system from advanced risks, threats, and vulnerabilities.

Overview

This screen displays information and controls connected to Malware Remover.



Running a Malware Scan

1. Open Malware Remover.

2.



Click
Malware Remover begins the scan.

3. Optional: After the scan finishes, click **View Logs** to view the results.


Running a Scheduled Scan

Scheduled scans periodically look for security threats on your QNAP device.



Note

The **Enable scheduled scan** checkbox is enabled by default.

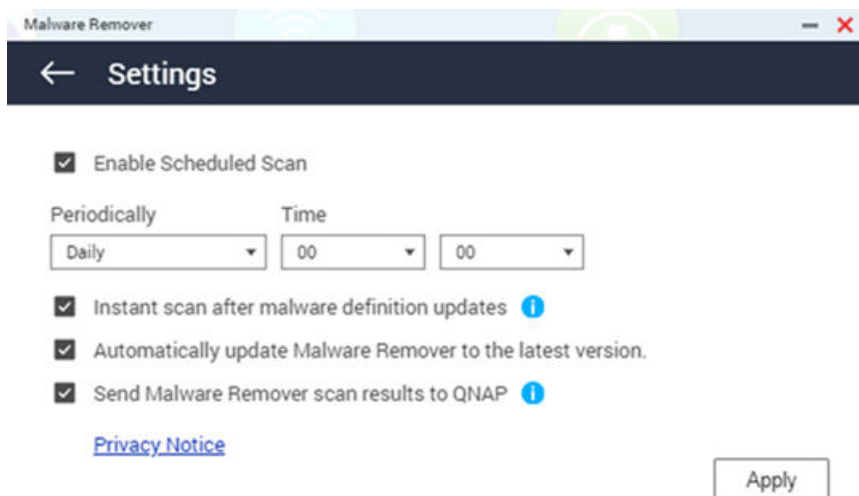
1. Open Malware Remover.
2. Click .
3. Choose from the scheduled scan drop-down menu to configure the settings.

| Setting | Description |
|---------|--|
| Daily | The scheduled scan runs daily at the specified time. |
| Weekly | The scheduled scan runs once a week on the specified day and time. |
| Monthly | The scheduled scan runs once a month on the specified date and time. |


4. Click **Apply**.

Settings

This screen contains the Malware Remover configuration options.



Configuring Malware Remover




1. Open Malware Remover.
2. Click .
The **Settings** window opens.
3. Configure the settings.

**Note**

All settings are enabled by default to prevent malware threats from infecting the system.

**Tip**

QNAP recommends running scans during off-peak hours.

| Setting | Description |
|---|--|
| Enable scheduled scan | <p>Enable to scan all applications and files at the user-configured frequency and time. For details, see Running a Scheduled Scan.</p> <p> Note Enabling this setting ensures Malware Remover performs routine scans of your device.</p> |
| Instant scan after malware definition updates | <p>Enable this option to run instant scans once Malware Remover updates the malware definitions.</p> <p> Note Malware Remover automatically updates malware signatures and security patches to have the most up-to-date security content.</p> |
| Send Malware Remover scan results to QNAP | <p>Enable this option to submit the scan results for malware analysis. QNAP collects the following data:</p> <ul style="list-style-type: none"> • NAS model • NAS IP address (The IP address is immediately deleted after analyzing the malware scan results.) • Scan status • Scan errors • Malware detection date and time • Malware ID <p> Note Disabling this option prevents Malware Remover from sending any data to QNAP.</p> |

4. Click **Apply**.

Malware Remover saves the settings.

19. Helpdesk


Helpdesk is a built-in application that allows you to quickly find solutions or contact the QNAP support team when you encounter any issues while using QTS and related applications.

Overview

On the **Overview** screen, you can contact the QNAP support team, browse frequently asked questions and application notes, download QNAP user manuals, find out how to use a QNAP NAS, search the QNAP knowledge base, and find compatible devices. This screen also displays Helpdesk message logs.

| Title | Description |
|---------------------------------------|--|
| Help Request | Contact the QNAP support team by submitting your issues or questions. |
| QNAP Online Tutorial & FAQ | Browse frequently asked questions and application notes for QNAP NAS and applications. |
| NAS User Manual | View or download QNAP NAS user manuals. |
| Help Center | Find how to use a QNAP NAS. |
| QNAP Helpdesk Knowledge Base | Search the QNAP knowledge base for answers from the support team for different issues. |
| Compatibility List | Find drives and devices that are compatible with QNAP NAS. |
| My Tickets | View your submitted tickets status. |

Configuring Settings

1. Open **Helpdesk**.
2. Go to **Overview**.
3. Click .
The **Settings** window appears.
4. Specify the message retention time.
5. Optional: Click **Retain all messages**.
6. Optional: Click **I am allowing QNAP Support to access my system logs**.
7. Optional: Click **Sign In**.
The **Settings** window appears.
8. Specify your QNAP ID.
9. Specify the password.
10. Click **Sign In**.
11. Click **Apply**.

Help Request

Help Request allows users to directly submit requests to QNAP from your NAS. Helpdesk automatically collects and attaches NAS system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

Submitting a Ticket

You can submit a Helpdesk ticket to receive support from QNAP. Helpdesk automatically collects and attaches device system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

1. Open **Helpdesk**.
2. Go to **Help Request**.
3. Sign in with your QNAP ID.
4. Specify the ticket details.

| Fields | User Actions |
|-------------------------|---|
| Subject | Specify the subject. |
| Issue Category | Select an issue category, and then select an issue. |
| Issue Type | Select an issue type. |
| Operating System | Select an operating system. |
| Description | Specify a short description for each issue. |


5. Upload the attachments.
 - a. Optional: Select **I am allowing QNAP Support to access my system logs**.
 - b. Upload screenshots or other related files.



Note

- You can upload up to 8 attachments, including system logs.
- Each file must be less than 5 MB.

6. Specify the following information.

| Fields | User Actions |
|--|--|
| Your Email Address | Specify your email address. |
| Phone number | Specify your phone number. |
| Customer type | Select a customer type. |
| Company name | Specify your company name.  Note This field only appears when you select Business User as the Customer type . |
| Your timezone | Select a timezone. |
| Apply the changes to my profile in QNAP Account | Click to apply your profile changes in QNAP Account. |
| First name | Specify your first name. |
| Last name | Specify your last name. |
| Your location | Select a location. |

7. Optional: Select **Apply the changes to my profile in QNAP Account**.

8. Click **Submit**.

Remote Support

Remote Support allows the QNAP support team to access your NAS directly to assist you with your issues.

Enabling Remote Support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Specify your ticket ID.
4. Specify your email address.
5. Click **Enable Remote Support**.
The **QNAP Helpdesk Terms of Service** window appears.
6. Accept the terms of service.
 - a. Click **I agree to these Terms of Service**.
 - b. Click **Agree**.
The **Enable Remote Support** window appears.



Note

Enable Remote Support is only required when you enable the feature for the first time.

7. Click **Confirm**.
Helpdesk creates a private key and temporary account.

Extending Remote Support

Extending Remote Support allows the users to extend the remote session by a week in case users want to have the remote session at a specific time. QNAP will also notify the user to extend the session if the issue is unsolved.

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Extend**.



Note

The **Extend** button only appears after Remote Support is enabled.

Disabling Remote Support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Disable**.



Note

The **Disable** button only appears after Remote Support is enabled.

4. Click **Finish**.



Note

Remote Support will also be disabled when the support team has completed the remote session, or when the private key has expired.

Diagnostic Tool

The Diagnostic Tool provides several features for checking the stability of the NAS. Users can export system kernel records to quickly check whether abnormal operations have recently occurred. In addition, users can send the records to QNAP technical support for further investigation. The Diagnostic Tool also provides features for checking the file system, hard drives, and RAM.

Downloading Logs

The Diagnostic Tool provides download log features for checking the device stability. You can export the system kernel records to quickly check for exceptions or errors that have occurred. In addition, you can send the records to QNAP technical support for further investigation.

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > Download Logs** .
3. Click **Download**.
Helpdesk generates a ZIP file.
4. Download the ZIP file.
5. Optional: Send the file to QNAP through Help Request for further investigation.

Performing an HDD Standby Test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > HDD Standby Test** .
3. Select an enclosure to analyze.
4. Click **Start**.
Helpdesk performs an HDD standby test.
5. Optional: Click **Download** to download the test reports.

Performing an HDD Stress Test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > HDD Stress Test** .
3. Click **Start**.
Helpdesk performs an HDD stress test.
4. Optional: Click **Download** to download the test reports.

20. Console Management

Console Management is a text-based tool that helps the admin account perform basic configuration or maintenance tasks, and provide technical support to the NAS users. The program is accessible only after the operating system has finished initialization. Console Management is enabled by default, but you can disable it in the Control Panel. For details, go to the System Settings section of the QTS User Guide. Currently, disabling Console Management only applies to QTS

Only the admin account can use Console Management, and it is automatically launched when the admin account logs in using SSH login, a serial console, or an HDMI monitor and a USB keyboard.

Enabling Secure Shell (SSH)

Secure Shell (SSH) is a cryptographic network protocol that can access Console Management. If you want to access Console Management using SSH, you must first enable SSH on the NAS.

Enabling SSH on the NAS

1. Log in to the NAS as the admin account.
2. Go to **Control Panel > Network & File Services > Telnet / SSH** .
3. Select **Allow SSH connection (Only administrators can login remotely.)**.
4. Optional: Change the port number.
5. Click **Apply**.

Enabling SSH on the NAS Using Qfinder Pro

1. Open **Qfinder Pro**, and then locate the NAS you want to access.
2. Click **Settings**.
3. Select **Connect via SSH**.
The **Connect via SSH** screen appears.
4. Log in to the NAS as the admin account.

Accessing Console Management

Before you can access Console Management, you must first enable SSH using the NAS or Qfinder Pro. A third-party software is also required on Windows platforms but not on Mac platforms.

Accessing Console Management from Windows

1. Download PuTTY from <https://www.putty.org/>, and then follow the on-screen instructions to install the software.
2. Open PuTTY, and type the device's IP address underneath **Host Name (or IP address)**.
3. Select **SSH** as the connection type.



Note

This option is selected by default.

- Click **Open**.
The **PuTTY Security Alert** window appears.

**Note**

This window only appears when you first run the application.

- Click **Yes**.
A login screen appears.

Accessing Console Management from Mac

- Open **Terminal**.
- Enter `ssh admin@NAS_IP`.

**Note**

Replace `NAS_IP` with the device's IP address.

**Tip**

If you encounter an error, enter `ssh-keygen -R NAS_IP`. Replace `NAS_IP` with the device's IP address.

- Press **ENTER**.
A login screen appears.

Logging In to Console Management

**Important**

Before performing this task, you must first complete the following tasks:

- Enable Secure Shell (SSH).
- Download the third-party software for your platform if it is required. For details, see the following topics:
 - [Accessing Console Management from Windows](#)
 - [Accessing Console Management from Mac](#)

- Log in as the admin account.
 - Enter the username.
 - Enter the password.

**Note**

For security purposes, the password does not show.

**Tip**

Do not copy and paste the password to the program.

The **Console Management - Main menu** screen appears.

Managing Existing Applications

- Log in to Console Management, and then enter 5.

The App window and three options appear.

2. Enter the alphanumeric character corresponding with the action you want to perform.




Tip

To browse your applications, enter **n** or **p** to go to the next or previous page.

| Option | User Action |
|----------------------------|---|
| List installed apps | Enter 1. Console Management displays a list of all installed applications on the operating system. |
| List enabled apps | Enter 2. Console Management displays a list of all enabled applications on the operating system. |
| List disabled apps | Enter 3. Console Management displays a list of all disabled applications on the operating system. |
| Return | Enter r . Console Management returns to Main menu. |

A list of applications appear.

3. Enter the alphanumeric character corresponding with the application you want to perform an action on. Five options appear.
4. Enter the alphanumeric character corresponding with the action you want to perform.

| Option | User Action |
|----------------|---|
| Start | Enter 1. The application starts. |
| Stop | Enter 2. The application stops. |
| Restart | Enter 3. The application restarts. |
| Remove | Enter 4. The application is removed.  Note If an application can't be removed, Console Management tells you that this function is currently unavailable. |
| Return | Enter r . Console Management returns to Main menu. |

The system performs the specified action and tells you whether the action has succeeded or not.

Activating or Deactivating a License

1. Log in to Console Management, and then enter 4.
Two options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

| Option | User Action |
|-----------------------------|--|
| Activate a License | <p>a. Enter 1.</p> <p>b. Enter a license activation key.</p> |
| Deactivate a License | <p>a. Enter 2.</p> <p>b. Enter a license activation key.</p> |
| Return | <p>Enter <i>r</i>.</p> <p>Console Management returns to Main menu.</p> |

The system performs the specified action.

Sorting and Filtering System Logs

1. Log in to Console Management, and then enter 2.
Eleven options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.



Note

System logs are displayed in the following format: record_id, date, time, user, app_id, application, category_id, category, msg_id, message.

| Option | User Action |
|---|--|
| date in ascending order | <p>Enter 1.</p> <p>Console Management displays all system logs in ascending order according to the date.</p> |
| date in descending order (default) | <p>Enter 2.</p> <p>Console Management displays all system logs in descending order according to the date.</p> |
| user in ascending order | <p>Enter 3.</p> <p>Console Management displays all system logs in ascending order according to the username.</p> |
| user in descending order | <p>Enter 4.</p> <p>Console Management displays all system logs in descending order according to the username.</p> |
| IP in ascending order | <p>Enter 5.</p> <p>Console Management displays all system logs in ascending order according to the IP address.</p> |
| IP in descending order | <p>Enter 6.</p> <p>Console Management displays all system logs in descending order according to the IP address.</p> |
| app name in ascending order | <p>Enter 7.</p> <p>Console Management displays all system logs in ascending order according to the application name.</p> |
| app name in descending order | <p>Enter 8.</p> <p>Console Management displays all system logs in descending order according to the application name.</p> |
| category in ascending order | <p>Enter 9.</p> <p>Console Management displays all system logs in ascending order according to the application category.</p> |

| Option | User Action |
|------------------------------|---|
| category in descending order | Enter 10. Console Management displays all system logs in descending order according to the application category. |

The filter screen appears.

3. Optional: Enter a filter query.



Note

- Ensure all filter conditions follow the relevant on-screen format. For example, filtering by an application name should follow this format: A={myQNAPcloud}.
- To filter by multiple conditions, use '&' in between filters. For example, filtering by severity level and an application name should follow this format: T={0} &A={myQNAPcloud}.

| Filter | User Action |
|------------------|---|
| Severity level | <p>a. Enter one of the following options.</p> <ul style="list-style-type: none"> • T={0} <p> Note This filter only includes system logs classified as information. This type of system log is indicated as in QuLog Center.</p> <ul style="list-style-type: none"> • T={1} <p> Note This filter only includes system logs classified as warnings. This type of system log is indicated as in QuLog Center.</p> <ul style="list-style-type: none"> • T={2} <p> Note This filter only includes system logs classified as errors. This type of system log is indicated as in QuLog Center.</p> <p>Console Management filters all system logs according to the specified severity level.</p> |
| Keyword | Enter a keyword. Console Management filters all system logs according to the specified keyword. |
| Username | Type an username. Console Management filters all system logs according to the specified username. |
| Source IP | Enter a source IP. Console Management filters all system logs according to the specified source IP. |
| Application name | Enter an application name. Console Management filters all system logs according to the specified application name. |
| Category name | Enter an application category. Console Management filters all system logs according to the specified category. |

A list of system logs appear.



Tip

To browse your applications, enter **n** or **p** to go to the next or previous page.

Showing Network Settings

1. Log in to Console Management as the admin account, and then enter **1**.



Note

Network settings appear in the following format: adapter, virtual switch, status, IP, MAC address.

The Network settings window appears.

Restoring or Reinitializing the Device

1. Log in to Console Management as the admin account, and then enter **3**.
The **Reset** window and five options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.



Note

The admin password is required to reset the settings or reinitialize the device.

| Option | User Action |
|--|--|
| Reset network settings | Enter 1 . Console Management resets the network settings. |
| Reset system settings | Enter 2 . Console Management restores system settings to default without erasing user data. |
| Restore factory defaults & format all volumes | Enter 3 . Console Management restores the system settings to default and formats all disk volumes. |
| Reboot to reinitialize the device | Enter 4 . Console Management erases all data and reinitializes the device. |
| Return | Enter r . Console Management returns to Main menu. |

Rebooting the NAS

You can reboot the NAS into rescue or maintenance mode from Console Management.

Rebooting the Device Into Rescue Mode

1. Log in to **Console Management** as the admin account, and then type **6** and press **ENTER**.
The **Reboot in rescue mode** window opens.
2. Type **y**, and then press **ENTER**.



Note

Press escape or type **n** and press to go to the **Main Menu**.

Console Management reboots the device.

Rebooting the Device Into Maintenance Mode

1. Log in to **Console Management** as the admin account, and then type `7` and press **ENTER**.
The **Reboot in maintenance mode** window opens.
2. Type `y`, and then press **ENTER**.
Press escape or type `n` and press to go to the **Main Menu**.
Console Management reboots the device.