



# **IEI QGW Series Software User Manual**

**(Version: 4.2.1)**

\*Unless otherwise specified, the content of this manual applies to all the QGW series models.

## Table of Content

Notice .....	4
Legal Notice and Trademarks .....	5
Document Annotation .....	6
Getting Started .....	8
Software Installation .....	10
Remote Installation .....	11
Local Installation .....	12
Getting Utilities .....	13
Connecting to Shared Folders .....	14
Windows .....	15
Mac or Linux.....	16
Connecting to the QGW Series by Web Browser .....	17
QTS Gateway Basics and Desktop .....	18
Introducing QTS Gateway.....	19
Using QTS Gateway Desktop .....	21
System Settings .....	27
General Settings .....	28
Storage Manager.....	31
Dashboard .....	34
Storage .....	36
Network .....	62
Security .....	73
Hardware.....	75
Power .....	77
Notification .....	79
Firmware Update .....	81
Backup/Restore .....	83
External Device .....	85
External Storage .....	86
USB Printer .....	89
UPS.....	96
System Status .....	99
System Logs.....	101
Privilege Settings.....	103
Users .....	104
User Groups .....	108
Shared Folders.....	109
Quota .....	119
Domain Security.....	120
Joining QGW to Active Directory (Windows Server 2003/2008/2012) .....	121
Connecting QGW to an LDAP Directory .....	123
Domain Controller.....	126
Network Services .....	134
Win/Mac/NFS .....	135
FTP.....	139
Telnet/SSH.....	141

SNMP Settings .....	142
Service Discovery .....	144
Network Recycle Bin .....	145
Qsync Central Station .....	147
Business Applications .....	157
Antivirus .....	158
Backup Station .....	162
Backup Server .....	163
Remote Replication .....	167
Snapshot Replica .....	174
Cloud Backup .....	176
External Backup .....	177
File Station .....	183
LDAP Server .....	197
SQL Server .....	199
NTP Service .....	201
RADIUS Server .....	202
Syslog Server .....	204
TFTP Server .....	207
Virtualization .....	208
VPN Client .....	210
VPN Server .....	213
Web Server .....	217
Virtual Host .....	220
Other Applications .....	222
App Center .....	223
DLNA Media Server .....	226
Download Station .....	227
HybridDesk Station .....	234
Multimedia Management .....	239
myQNAPcloud Service .....	241
Photo Station .....	249
Station Manager .....	263
Transcode Management .....	265
Video Station .....	267
Mobile Apps .....	277
Computer Utilities .....	282
NAS Add-ons .....	284
GNU GENERAL PUBLIC LICENSE .....	290

# Notice

[Legal Notice and Trademarks](#)

[Document Annotation](#)

# Legal Notice and Trademarks

## **Legal Notices**

The information in this document is subject to change without prior notice in order to improve reliability, design and function and does not represent a commitment on the part of the manufacturer.

In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

## **Trademarks**

All registered trademarks and product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

# Document Annotation

## Annotations in this document

***Warning:*** This indicates the instructions must be strictly followed. Failure to do so could result in injury to human body or death.

***Caution:*** This indicates the action may lead to disk clearance or loss OR failure to follow the instructions could result in data damage, disk damage, or product damage.

***Important:*** This indicates the information provided is important or related to legal regulations.



# Getting Started

New users are advised to follow the below steps to complete their installation.

1. [Software Installation](#)
2. [Getting Utilities](#)
3. [Connecting to the Shared Folders](#)
4. [Connecting to the QGW series by Web Browser](#)

## Alarm Buzzer

The alarm buzzer can be disabled in "Control Panel" > "System Settings" > "Hardware" > "Buzzer".

Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	<ol style="list-style-type: none"><li>1) The QGW series is starting up.</li><li>2) The QGW series is being shut down (software shutdown).</li><li>3) The user presses the reset button to reset the QGW series.</li><li>4) The system firmware has been updated.</li></ol>

# Software Installation

After installing the HDDs to the QGW series, proceed to software installation. There are three approaches for software installation:

1. [Remote Installation](#)
2. [Local Installation](#)

## Remote Installation

Follow the steps in this section to complete software installation for the QGW series from a remote console:

1. Install the Qfinder Pro from the product CD-ROM (or download the Qfinder Pro from <http://www.ieiworld.com>).
2. Run the Qfinder Pro to search for the QGW series. If the Qfinder Pro is blocked by your firewall, unblock the utility.
3. Double click on the QGW series in Qfinder Pro. The built-in Qfinder Pro Setup Wizard will guide you along the way to complete firmware installation. Next, you can use QTS Gateway account username and password to log in (QTS Gateway is the operating system for the QGW series.)

**Note:**

The default login ID and password of the QGW series are both "admin".

## Local Installation

Follow the steps in this section to complete the local software installation for the QGW series:

1. Connect the QGW series to a display device.
2. Follow the onscreen instructions to complete the firmware installation.
3. Choose to install [HD Station](#) or log into QTS Gateway with QTS Gateway account username and password (QTS Gateway is the operating system for the QGW series.)

**Note:**

The default login ID and password of the QGW series are both "admin".

# Getting Utilities

IEI has prepared a number of practical and useful utilities to enhance your using experience. After setting up the system, choose from the following two methods to install the utilities:

## **Method 1: Downloading from the website**

Visit <http://www.qnap.com/> and go to "Support" > "Download" > "Utilities" and choose to download and install the utilities on your PC.

## **Method 2: Installing from the product CD-ROM**

If the QGW series contains a CD-ROM, then it will contain: Qfinder Pro, myQNAPcloud Connect and NetBak Replicator.

Browse the CD-ROM and access the following contents:

- Quick Installation Guide: View the QGW series hardware installation instructions.
- Install Qfinder Pro: This will install Qfinder Pro for Windows.
- Install myQNAPcloud Connect: This will install myQNAPcloud Connect for Windows.
- Install NetBak Replicator: This will install NetBak Replicator - a backup utility for Windows.)
- User Manual and Application Notes: Instructions for installing and using the QGW series.

# Connecting to Shared Folders

After installing the hardware and software, it is time to connect to the shared folders on the QGW series. Refer to these links for the connection setup:

- [Connecting to the shared folders in Windows](#)
- [Connecting to the shared folders in Mac or Linux](#)

# Windows

There are two methods for connecting to shared folders of the QGW series when using Windows:

## **Method 1: Connect to the shared folders of the QGW series by using Qfinder Pro**

1. Launch Qfinder Pro. Select your QGW series and then click "Tool" > "Map Network Drive".
2. Select a shared folder on the QGW series to be mapped as a network drive and click "Map Network Drive".
3. Enter the username and password to connect to the QGW series and click "OK".
4. Select a drive in the OS to map the folder chosen in Step 2 and click "Finish".
5. The mapped folder will appear when opening the File Explorer in Windows.

**Note:** Alternatively, you can use the Storage Plug & Connect Wizard to connect to the shared folders. The steps:

1. Launch Qfinder Pro;
2. Select "Storage Plug & Connect" under "Connect";
3. Check "Login with username and password" and enter the username and password;
4. Click a shared folder;
5. Click "Map the Network Drive".

## **Method 2: Connect to the shared folders of the QGW series by using File Explorer or Run**

1. Open the Windows File Explorer, click on "Network" on the left and find the workgroup of the QGW series. If the QGW series system cannot be found, browse the whole network to search for the QGW series. Double click the name of the QGW series to connect to it, or use the Run function in Windows (Windows key + R). Enter \\QGW\_name or \\QGW\_IP.
2. Enter the default administrator name and password (the default login ID and password are both "admin".).
3. Upload files to the shared folders.

# Mac or Linux

## Mac Users

There are two methods to connect shared folders on a QGW series system:

### Method 1: Using Qfinder Pro

1. Launch Qfinder Pro, select your QGW series system, and go to "Connect" > "Open in File Explorer".
2. Enter your login ID and password.
3. Select the folder you want to mount and click "OK".
4. The folder is mounted.

### Method 2: Connecting to Server

1. Choose "Go" > "Connect to Server".
2. Enter the IP address of the QGW series.
3. Enter your login ID and password.
4. Select the folder you want to mount and click "OK".
5. The folder is mounted.

## Linux Users

On Linux, run the following command:

```
mount -t nfs <QGW System IP>: /<Shared Folder Name> <Directory to Mount>
```

For example, if the IP address of the QGW series is 192.168.0.1, to connect to the shared folder "public" under the /mnt/pub directory, use the following command:

```
mount -t nfs 192.168.0.1: /public /mnt/pub
```

Log into the QGW series with the specified user ID, use the mounted directory to connect to the shared folders.

**Note:** You must login as the "root" user to initiate the above command.

# Connecting to the QGW Series by Web Browser

To connect to the QGW series by a web browser, follow these steps:

1. Enter `http://QGW System IP:8080` in the web browser. Or if using Qfinder Pro, simply double click on the QGW series to open the login page.

**Note:** The default IP is 169.254.100.100:8080. If the QGW series has been configured to use DHCP, you can use Qfinder Pro to check the IP address of the QGW series. Make sure the QGW series and the computer that runs Qfinder Pro are connected to the same subnet. If the QGW series cannot be found, connect the QGW series to the computer directly and run Qfinder Pro again.

2. Enter the administrator's login id and password. Enable "Secure login" (Secure Sockets Layer login) to allow a secure connection to the QGW series system. If a user without administration rights logs into the QGW series system, the user can only change the login password (the default login ID and password of the QGW series are both "admin".)

**Note:** If the QGW series is behind a NAT gateway, to connect to the QGW series by secure login on the Internet, port 443 must be opened on the NAT router and forwarded to the LAN IP of the QGW series.

3. The QGW series Desktop will be displayed.

# QTS Gateway Basics and Desktop

QTS Gateway is a user-friendly operating system designed to enhance every aspect of your using experience. With basic methods such as drag-and-drop or point and click, you can complete most operations. Check the following links to learn more about QTS Gateway:

- [Introducing QTS Gateway](#)
- [Using QTS Gateway Desktop](#)

# Introducing QTS Gateway

Built on a Linux foundation, QTS Gateway is shaped from an optimized kernel to deliver high-performance services that satisfy needs for file storage, management, backup, multimedia applications, surveillance, and more. The intuitive, multi-window and multi-tasking QTS Gateway GUI make it incredibly easy to manage your QGW series system, use its rich industrial applications, and install more applications from an integrated App Center. QTS Gateway also adds value to business applications and effectively increase business efficiency with abundant features, including file sharing, virtualization, backup, privilege settings, and more. Coupled with various utilities and smart mobile apps, QTS Gateway is the ultimate platform for building a personal or private cloud, synchronizing data and sharing files.



## For Business - Efficiently optimize business IT infrastructure

IT efficiency, coupled with low total cost of ownership (TCO) is an essential factor for business competitiveness. IEI QGW series features advanced capabilities for keeping businesses running at maximum efficiency including business-critical applications, seamless file sharing, easy integration into existing networks, flexible virtualized IT environments, and more. Learn more about the compelling features that a IEI QGW series system offers your business:

- Large data storage, backup and file sharing center
- Supports both scale-up and scale-out solutions for growing data needs

- Advanced storage management with dynamic thin-provisioning and SSD caching expansion functions
- Trustworthy data security and data encryption
- Reliable IP SAN storage as primary and secondary storage for virtualization environments
- Private cloud storage
- Free and large capacity for Dropbox-style data sync
- Hundreds of install-on-demand applications from the App Center
- Development Center for third-party partners to build apps for the QGW series

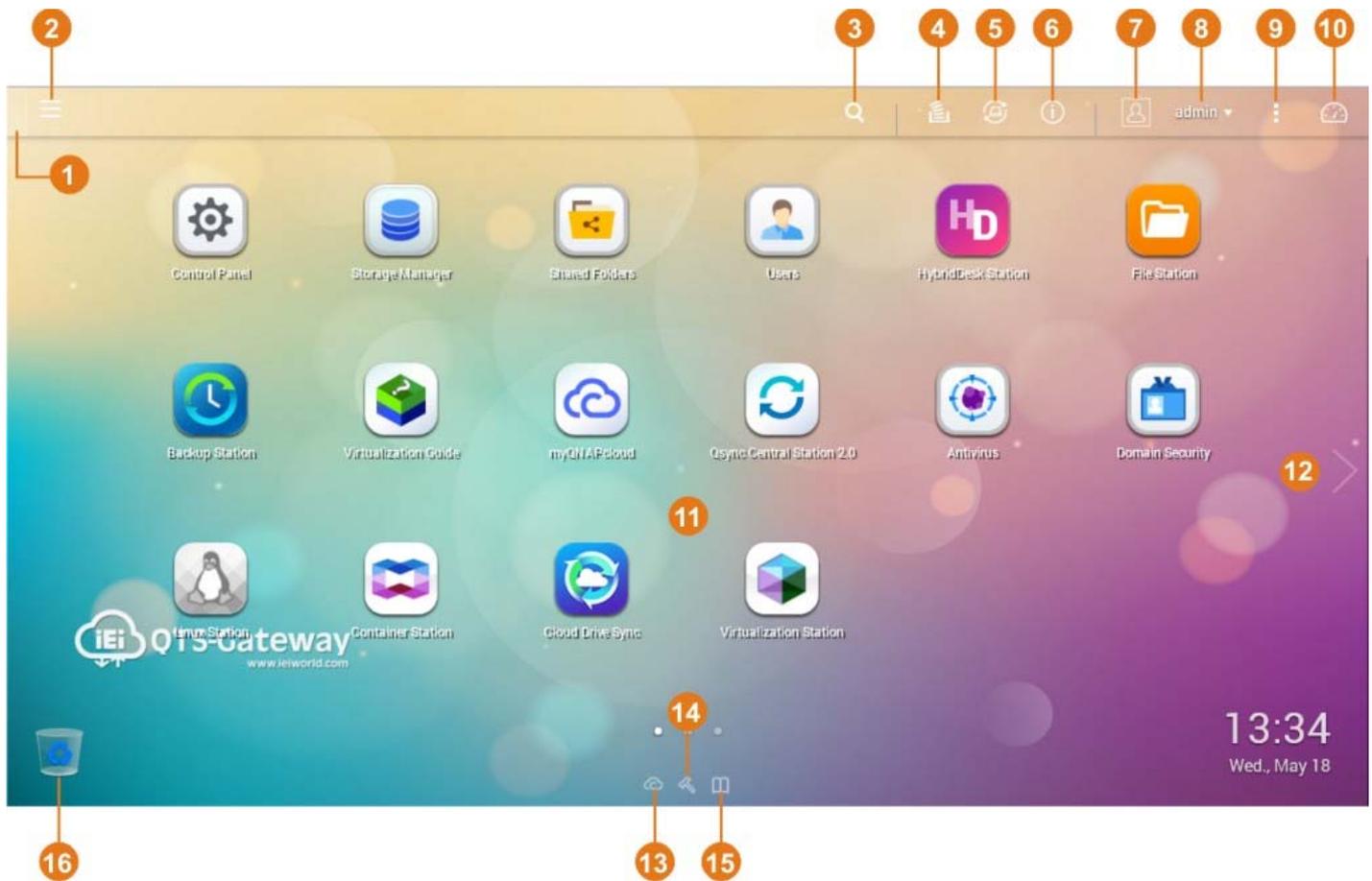
# Using QTS Gateway Desktop

After you finish the basic setup and login to the QGW series, the desktop will appear. Each main desktop feature is introduced in the following sections.

Topics covered in this chapter:

- [QTS Gateway Desktop](#)
- [2-step Verification](#)

## QTS Gateway Desktop



NO.	Name	Description
1	Show Desktop	Minimizes/restores all open windows.
2	Main Menu	Show the Main Menu. It includes two parts: 1) System features and settings (SYSTEMS): Key system features designed to manage or optimize the QGW series; 2) Applications: Applications developed by QNAP to enhance your using experience;

3	Search	Enter a feature specific keyword in the search bar to search for the desired function and its corresponding online help. Click the result in the search bar to launch the function or open its online QTS Gateway help.
4	Background Task	Review and control (including pausing or postponing) all tasks running in the background (such as HDD SMART scanning, antivirus scanning, file backup or multimedia conversion.)
5	External Device	List all external storage devices and USB printers that are connected to the QGW series via its USB or SATA ports. Click a listed device to open the File Station for that device. Click the "External Device" header to open the External Device page for relevant settings and operations (for details on File Station, refer to the File Station chapter.) Click the eject icon (up-arrow icon) to eject the external device.
6	Notification and Alert	Check for recent system error and warning notifications. Click "Clear All" to clear the list. To review all historical event notifications, click the "Event Notifications" header to open the System Logs. For details on System Logs, refer to the <a href="#">System Logs</a> chapter.
7	Options	<ul style="list-style-type: none"> <li>• Profile: Specify your email address and change your profile picture. You can also check <a href="#">System Logs</a> and edit the <a href="#">Login Screen</a> here.</li> <li>• Wallpaper: Change the default wallpaper or upload your own wallpaper.</li> <li>• 2-step Verification: Enable 2-step Verification to enhance the security of user accounts. For details, refer to the <a href="#">2-step Verification</a> section.</li> <li>• Change Password: Change your login password.</li> <li>• E-mail Account: Set the email address to use when sharing files via email in Photo Station, Video Station, or File Station.</li> <li>• Miscellaneous: <ul style="list-style-type: none"> <li>○ Auto logout after an idle period of: Specify the idle period before the current user is automatically logged out.</li> <li>○ Warn me when leaving QTS Gateway: Users will be prompted for confirmation each time they leave the QTS Gateway Desktop (such as clicking the browser back button or close the browser.) It is advised to check this option.</li> <li>○ Reopen windows when logging back into QTS Gateway: Check this option, and all the current desktop settings (such as the "windows opened before your logout") will be kept after your next login.</li> <li>○ Show the desktop switching button: Check this option to hide the next desktop button (No. 12) and only display them when you move your mouse cursor close to the buttons.</li> <li>○ Show the link bar on the desktop: Uncheck this option to hide the link</li> </ul> </li> </ul>

		<p>bar (No. 13, No. 14 and No. 15.)</p> <ul style="list-style-type: none"> <li>○ Show the Dashboard button: Uncheck this option to hide the Dashboard button (NO. 10).</li> <li>○ Show the time on the desktop: Uncheck this option to not display the time in the bottom-right of the desktop.</li> <li>○ Keep Main Menu open after selection: Keep the Main Menu pinned/unpinned on the desktop.</li> <li>○ Show a list of actions when external storage devices are detected: Uncheck this option and the Autoplay dialog box will not appear after you plug in an external device.</li> </ul>
8	Admin Control	<p>Customize user-specific settings, change your user password, restart/shut down the QGW series or log out your user account.</p> <ul style="list-style-type: none"> <li>• Last login time: The time the system was last logged in.</li> <li>• Options: Refer to No. 7 above.</li> <li>• Restart: Restart your QGW system.</li> <li>• Shutdown: Shut down your QGW system. <ul style="list-style-type: none"> <li>○ <b>Note: To power off a QGW series system, you can also: Run Qfinder Pro and click "Tools" &gt; "Shut down Server".</b></li> </ul> </li> <li>• Logout: Log yourself out</li> </ul>
9	More	<ul style="list-style-type: none"> <li>• Help: Display a list of online references, including the Quick Start Guide, QTS Gateway Help and Tutorials.</li> <li>• Language: Choose your preferred language for the UI.</li> <li>• Desktop Preference: Choose the application icon display style and select your preferred application opening mode on the desktop. Application icons can be switched between small and detailed thumbnails. Applications can be opened in Tab Mode, Window Mode, or Frameless Mode. Only Tab Mode is available if you log into the QGW series using a mobile device. <ul style="list-style-type: none"> <li>○ Tab Mode: In this mode, the window will be opened to fit the entire Desktop and only one application window can be displayed at a time.</li> <li>○ Window mode: In this mode, the application window can be resized and reshaped to a desirable style.</li> <li>○ Frameless Mode: In this mode, applications will be opened without their frames.</li> </ul> </li> <li>• Feedback: File a feature request and bug report.</li> <li>• About: Check the QGW series model, firmware version, HDDs already installed and available (empty) bays.</li> </ul>
10	Dashboard	<p>Check important QGW system statistics, including system and HDD health, resources, storage usage, online users, scheduled tasks, etc. Click the header</p>

		within each widget to open its respective page.
11	Desktop Area	Remove or arrange all applications on the desktop, or drag one application icon over the top of another to put them in the same folder.
12	Next Desktop/ Last Desktop	Switch between desktops.
13	myQNAPcloud	Go to the <a href="#">myQNAPcloud website</a> .
14	Utility	Check and download the latest and available QGW system utilities.
15	Feedback	File a feature request and bug report.
16	Network Recycle Bin	All of the deleted items can be found in here. Right click on it to open the Network Recycle Bin, empty it (or permanently delete), or configure it (refer to the <a href="#">Network Recycle Bin</a> chapter for details.)

## 2-step Verification

2-step Verification enhances the security of user accounts. Once enabled, you will need to enter a one-time security code (6 digits) in addition to your password whenever you sign in to the QGW series. 2-step verification requires a mobile device with an authenticator app which supports the Time-based One-Time password (TOTP) protocol. Supported apps include Google Authenticator (Android/iPhone/BlackBerry) or Authenticator (Windows Phone.)

### Start 2-step verification

1. Install the authenticator App on your mobile device: For Android and iOS devices, install the Google Authenticator App from their respective App stores. For Windows Phone, install the Authenticator from its Store.
2. The system times of your mobile device and QGW series must be synchronized. It is recommended to use the time provided from the Internet.
3. Go to "Options" > "2-step Verification" and click "Get Started". Complete the steps in the wizard to set up the QGW series and your mobile device.
4. Configure your authenticator App by scanning the QR code or by entering the Secret Key into the App.
5. Enter the code generated from the app to the QGW series to verify the correct configuration.
6. Select an alternative verification method by emailing you a security code or by answering a security question if you cannot use your mobile device. To email a security code, the SMTP server must be properly configured in "Control Panel" > "Notification" > "E-mail".

## Sign in QTS Gateway with 2-step verification

After your username and password are verified, you will be promoted to enter a security code. Enter the code currently provided from the authenticator app to sign in to QTS Gateway. If you cannot use your mobile device or your device is lost, you can select "Verify another way" to sign in with your chosen alternative verification method.

## Stop 2-step verification

If you want to disable 2-step verification, go to "Options" > "2-step Verification" and click "Stop". Administrators can disable 2-step verification for other account users if they are locked out by going to "Control Panel" > "Users" > "Edit Account Profile"

If an administrator cannot use a mobile device to sign in to QTS Gateway and no other administrators are available to disable 2-step verification for the locked-out administrator, the QGW series must be restored to factory settings by physically pressing the clear CMOS button inside the QGW series.

### Tip:

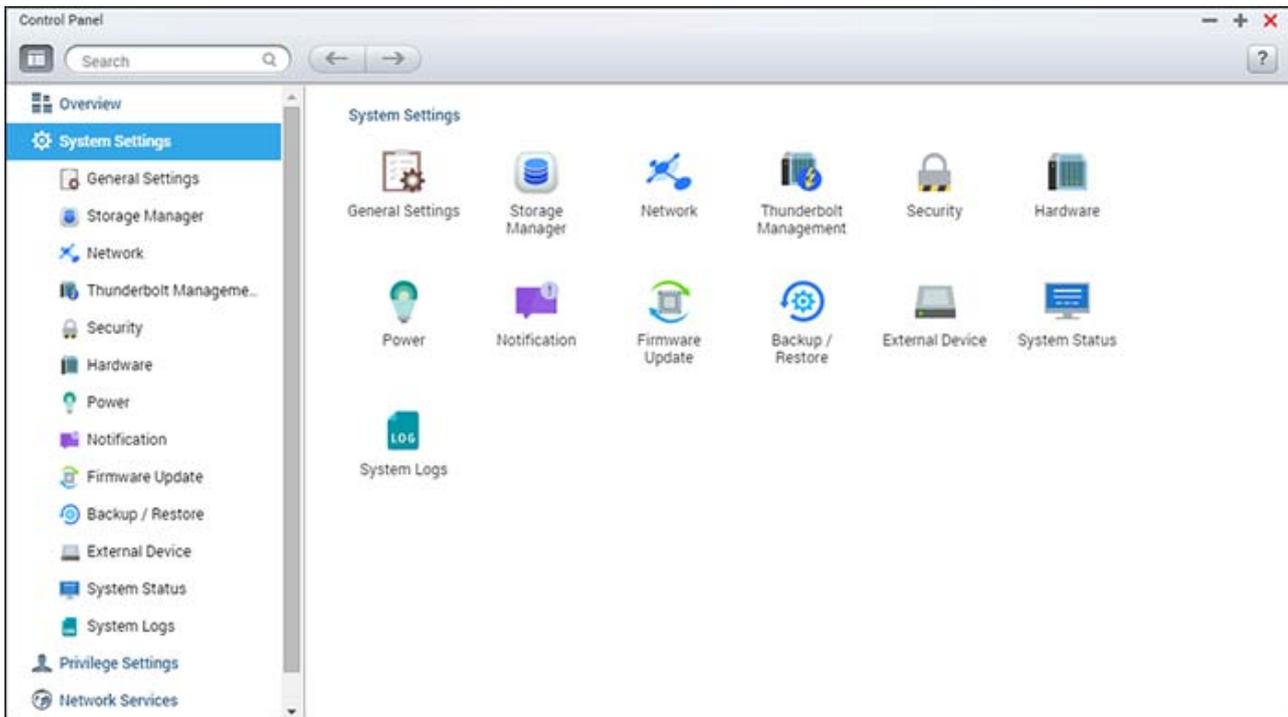
- All of the Dashboard widgets can be dragged onto the desktop for monitoring specific details.
- The Dashboard will be presented differently on different screen resolutions.
- The color of the Dashboard button will change based on the status of system health for quick recognition.

**Note:** The recommended minimum screen resolution for QTS Gateway 4.2 is 1024x768.



# System Settings

Go to "Control Panel" > "System Settings" to set up your QGW series.



For details on the settings, refer to the following links:

- [General Settings](#)
- [Storage Manager](#)
- [Network](#)
- [Security](#)
- [Hardware](#)
- [Power](#)
- [Notification](#)
- [Firmware Update](#)
- [Backup/Restore](#)
- [External Device](#)
- [System Status](#)
- [System Logs](#)

# General Settings

Go to "Control Panel" > "System Settings" > "General Settings" to configure basic settings of the QGW series.

The screenshot shows the 'General Settings' page for a QGW series device. The 'System Administration' tab is selected. The 'Server name' is set to 'NASC4EF14'. The 'System port' is set to '8080'. The 'Enable secure connection (HTTPS)' checkbox is checked, and the 'Port number' for HTTPS is set to '443'. The 'Force secure connection (HTTPS) only' checkbox is unchecked. A note indicates that enabling the 'Force secure connection (HTTPS) only' option restricts access to HTTPS. There are 'Apply' and 'Apply All' buttons at the bottom.

Topics covered in this chapter:

- [System Administration](#)
- [Time](#)
- [Daylight Saving Time](#)
- [Codepage](#)
- [Password Strength](#)
- [Login Screen](#)

## System Administration

- **Basic Settings:** Enter the name of the QGW series. The QGW system name supports maximum 14 characters and can be a combination of letters (a-z, A-Z), numbers (0-9), and dash (-). Space ( ), period (.), or pure numbers are not allowed. Enter a port number for system management. The default port is 8080. The services which use this port include: System Management, Photo Station, File Station and Download Station. If you are not sure about this setting, use the default port number.
- **Enable Secure Connection (HTTPS):** Allows users to connect to the QGW series by HTTPS. Enable secure connection (HTTPS) and enter the port number. If the option "Force secure connection (HTTPS) only" is enabled, users can only connect to the web administration page by HTTPS.

## Time

- **Basic time settings:** Adjust the date, time, and time zone according to the location of the QGW series. If the settings are incorrect, the following problems may occur:
  - When using a web browser to connect to the QGW series or save a file, the display time of the action will be incorrect.
  - The time of the event logs will be inconsistent with the actual time when an action occurs.
- **Manual Setting:** To synchronize the time of the QGW series with the computer time, click "Update now" next to this option.
- **Synchronize with an Internet time server automatically:** Enable this option to synchronize the date and time of the QGW series automatically with an NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, for example, time.nist.gov, time.windows.com. Then enter the time interval for synchronization. This option can be used only when the QGW series is connected to the Internet.

**Note:** First time synchronization may take several minutes to complete.

## Daylight Saving Time

If your region uses daylight saving time (DST), enable "Adjust system clock automatically for daylight saving time" and click "Apply". The latest DST schedule of the time zone specified in the "Time" section will be shown. The system time will be adjusted automatically according to the DST. Note that if your region does not adopt DST, the options on this page will not be available. To manually enter the DST table, select the option "Enable customized daylight saving time table". Click "Add Daylight Saving Time Data", enter the daylight saving time schedule, and click "Apply" to save the settings.

## Codepage

Select the language the QGW series uses to display files and directories.

**Note:** All of the files and directories on the QGW series use Unicode encoding. If your FTP clients or PC OS does not support Unicode, select the language which is the same as the OS language in order to properly view files and directories on the QGW series.

## Password Strength

Specify the password rules. After applying the setting, the QGW series will automatically check the validity of the password.

## Login Screen

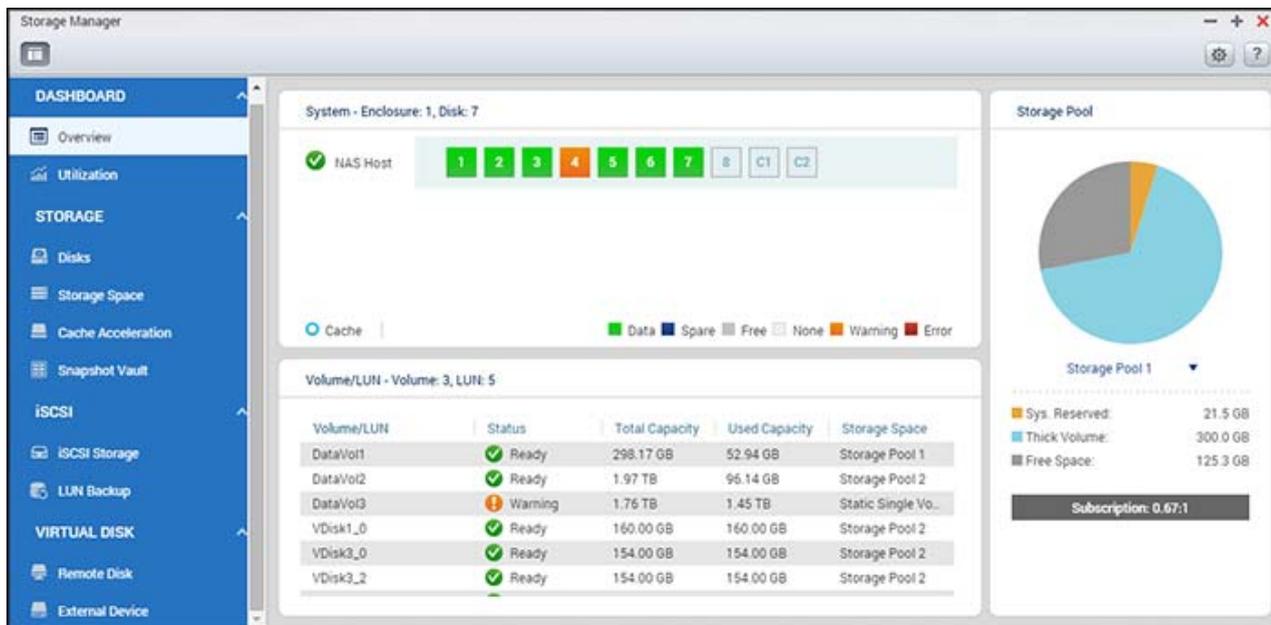
Set the login screen style. Settings available on this page include:

- Login screen template: Select the preferred login screen style. If you choose the classic login screen style, you can click "Preview" at the bottom before applying your settings.
- Show firmware version: Show the firmware version on the login page.
- Show the link bar: Show/hide shortcut links (QNAP utilities, myQNAPcloud portal site, and Feedback) on the login screen.
- Photo Wall: This part of the settings is only for the Photo Wall style login screen. Enter a personal message and choose to randomly select 100 photos stored on the QGW series or display 100 photos that were recently shared. Click "Change Picture" to set a picture for your profile photo on the photo wall. Or use your profile picture. Click "Preview" to preview the photo wall login screen or "Apply" to apply the settings. To change the pictures shown on the photo wall, check the [Creating and managing album](#) section.

After you finish the above settings, click "Preview" to preview the chosen template or "Apply" to apply the chosen login screen.

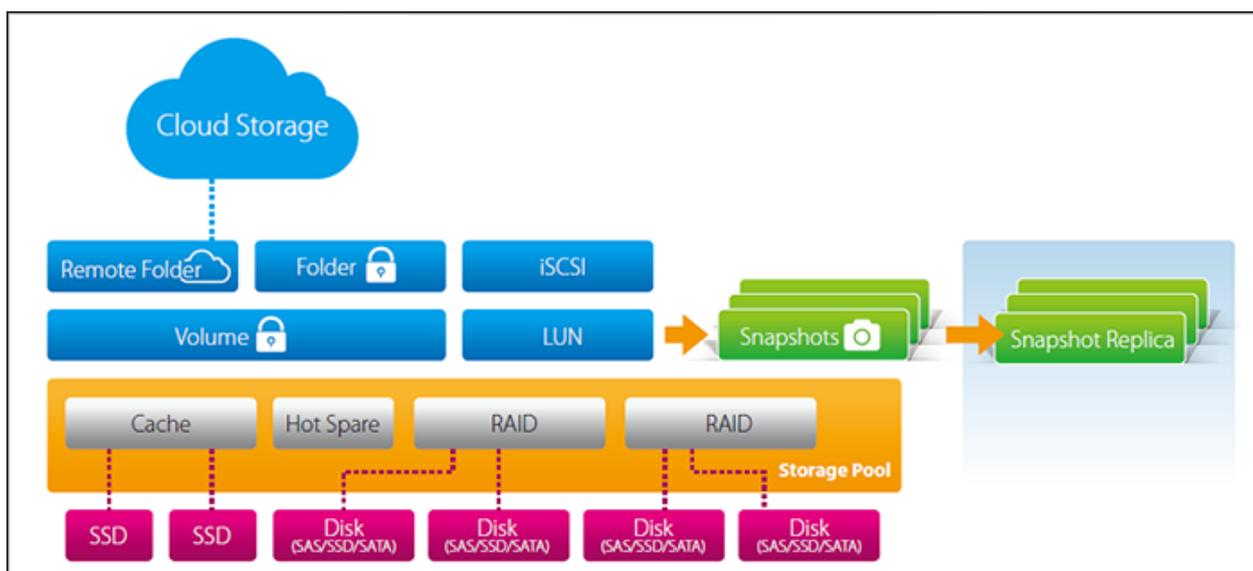
# Storage Manager

Based on the Flexible Volume Architecture, the Storage Manager provides a secure, flexible and comprehensive approach to manage data on your QGW series and offers a number of great features such as storage pools, multiple RAID groups, thin-provisioned volumes, space reclamation, and online capacity expansion. These features can effectively protect your storage system and your valuable data.



## Flexible Volume Architecture

The Flexible Volume Architecture consists of the following four layers: HDD Management, Storage Pool, Volume and Shared Folders, as shown below:



Each layer is designed to cover an aspect of the storage system, and all four layers combined can achieve total protection for your storage system.

This architecture supports four distinct types of volumes, and each volume type supports different storage features:

Features	Legacy volume	Static Volume	QTS Gateway 4.2
			Storage Pool Flexible Volume
Performance level	High	High	Medium
Online RAID migration	●	●	●
Online RAID expansion	●	●	●
File-based LUN	●	●	●
Block-based LUN			●
Thin provision			●
SSD cache		●	●
Snapshot			●
Snapshot Replica			●
Snapshot Vault			●

For specific setup of the Storage Manager, please refer to the following links:

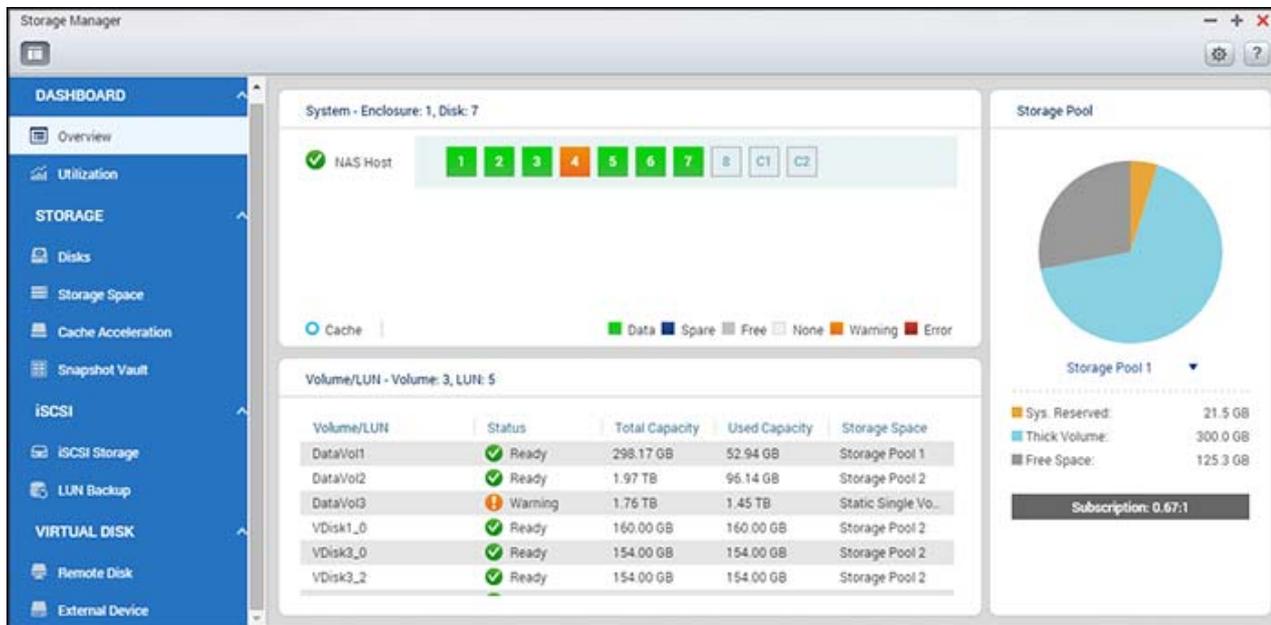
- [Dashboard](#)
- [Storage](#)

**Note:**

To expand storage space with an expansion unit connected via a USB cable, you must create a separate static volume or storage pool on the expansion unit. Expanding an existing storage pool to an expansion unit is not supported.

# Dashboard

The Storage Manager dashboard provides an overview for IT administrators to easily monitor and manage storage allocations.



## Overview

There are three sections on the page: Disk, Volume/LUN and Storage Pool. They are described below:

- **Disk:** The physical hard disk drives and their associated storage hosts (including both the QGW series and its connected expansion enclosures) are shown in this section. Click the hard disk drive icon to bring up the Disk Health window. For details on the Disk Health window, please refer to the [Disks](#) chapter.
- **Volume/LUN:** All available logical volumes, their capacity and type (Volume, LUN and Unused) are listed in this section. For details on volumes and LUN, please refer to the [Volumes](#) chapter.
- **Storage Pool:** This section provides a space usage overview on the storage pool created on the QGW series. You can check the space distribution on the pie chart for each storage pool (including the size of reserved system space, thick volume and free space) and its subscription. Subscription is the ratio between claimed space and available space in the storage pool. If a user creates a thin-provisioned volume with 10TB claimed space, while the available space is only 1TB, the "Subscription" value in the "Overview" page will be 10:1, meaning that the thin-provisioned space is oversubscribed and users must note that the available space in storage pool is too low. You can also click on the down arrow next to the storage pool to switch between storage pools. For details on storage pools, please refer to the [Storage Pools](#) chapter.

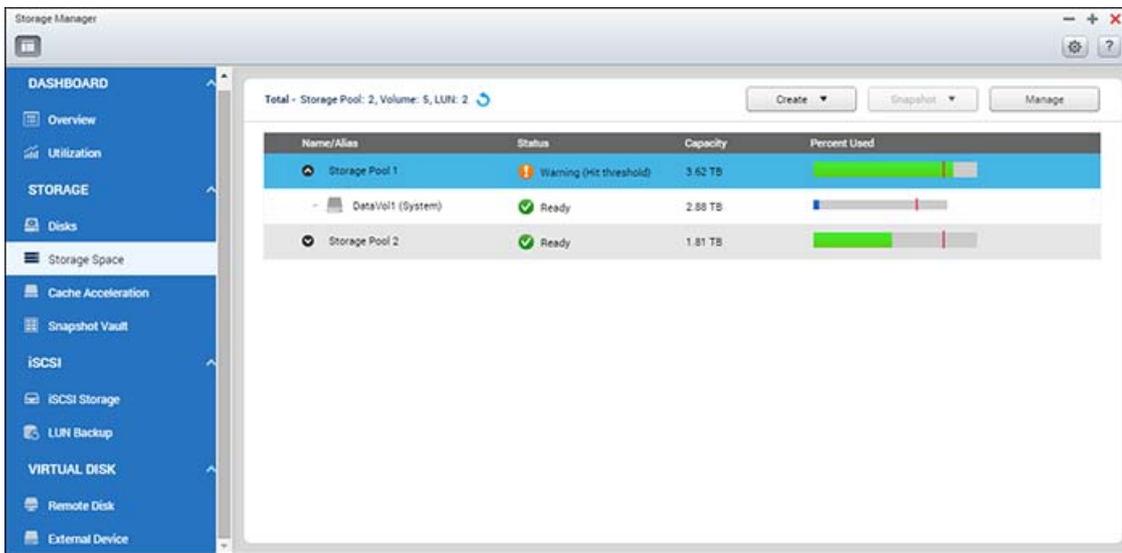
## Utilization

This page is designed for users to monitor storage utilization of their QGW series system. With volume and storage pool usage information presented on this page, users can manage their storage system more effectively and spot potential issues based on trends over a period of time (from the last hour to the last year.)

Select to view the storage usage rate of a particular volume or storage pool and specify the period. Click "Clear Record" to reset the utilization graph.

# Storage

Manage volumes, storage pools, hard disk drives, snapshots, encrypt and decrypt file systems, and configure cache acceleration with Storage Manager.



For details on the features, refer to the following links:

- [Disks](#)
- [Storage Space](#)
- [Cache Acceleration](#)
- [Snapshot Vault](#)

## Disks

This page is designed for users to monitor and manage hard disk drives installed on the QGW series and its connected expansion enclosures, and users can quickly isolate and identify hard drives for relevant maintenance tasks.

### Managing NAS Hosts

Click a QGW system under "NAS Host" in the system component panel to check its general information. Refer to the following table for actions available to manage a NAS host:

Action	Description
Enclosure Info	Click this button to check details of an enclosure, including the model, serial number, firmware version, BUS type, BIOS version, CPU temperature, system temperature, power status, system fan speed and power fan speed.
Locate (under "Action")	Click this button and the chassis LEDs of the selected NAS host will blink for easy identification.
RAID Group	Click this button and select a RAID group to check its details, including capacity, RAID group name, RAID type and disk member.

### Managing Disks

Click "+" beside the NAS host in the system component panel and select a disk to check its general information. The legend shown under the system component panel is provided to indicate the types of hard disk drives:

- Cache: A disk drive configured as cache.
- Data: A disk drive that contains data.
- Free: An empty disk drive that does not have any data on it.
- Spare: A disk drive configured as spare drive for a RAID group.
- Error: A disk drive detected with errors (could be bad sectors or I/O errors) and it is recommended that this disk drive is to be replaced immediately.
- Warning: A disk drive is approaching failure.

Refer to the following table for actions available to manage a disk:

Action	Description
Disk Info	Click this button to check details of a disk, including the model, model number, serial number, capacity, firmware version, ATA version and ATA

	standard.
Disk Health	Click this button to check disk S.M.A.R.T information. More details about S.M.A.R.T information will be provided in the next table.
Scan Now (under "Action")	<p>Click this button to scan the disk for bad blocks. If bad blocks are found, the number of bad blocks will be displayed in the "Status" field. Check the bad block sectors by clicking on the "bad blocks" message so long as the disk is not busy.</p> <p>You can also use this function if a drive is in an error state. In this case, if no bad blocks found after a complete scan, the error state of drive will be changed back to normal.</p>
Locate (under "Action")	Click this button to locate drives using LED lights for easy identification of physical hard drives.
Set as Enclosure Spare (under "Action")	Click this button to set the chosen hard disk drive as an enclosure spare drive in RAID 1. In case a spare drive is shared by multiple RAID groups, that spare drive will be used to replace the first failed drive across all RAID groups. Please note that the capacity of the enclosure spare drive must be equal to or larger than that of the member drive in a RAID group and this option is only available for an empty disks. Note that an enclosure spare can only be used within an enclosure.
Disable Spare (under "Action")	Click this button to cancel the chosen hard disk drive as an enclosure spare drive.
New Volume (under "Action")	Click this button to create a new volume. For details, please refer to the chapter on <a href="#">Volumes</a> .
RAID Group	Click this button and select a RAID group and check its details, including capacity, RAID group name, RAID type and disk member.
View Mode (located above the system component panel)	<p>Switch to list view using the list view icon on top-left of the page. In the list view, you can show or filter for disks. Set the filter from the drop down list to only show hard disks based on the device (enclosure or QGW series system they belong to), model, type (HDD or SSD), BUS type, capacity, used type (data, free, error, spare, cache, or none) and status. Click "Refresh" to refresh the list.</p> <p>You can also perform sequential read and IOPS read tests (under "Performance test"), schedule weekly sequential read tests, and check</p>

	the test results to gauge the performance of the tested disks.
--	--

**HDD S.M.A.R.T Information**

Switch to the icon view (or tree view) and click the "Disk Health" button to bring up the Disk Health window.

First select the NAS Host or an expansion enclosure and one of its disks to check for S.M.A.R.T information. Refer to the below table for descriptions of each field:

Field	Description
Summary	This page provides an overview on hard disk S.M.A.R.T details and the result of the latest test.
Hard Disk Information	This page shows hard disk details, including disk model, model number, serial number, disk capacity, firmware version, ATA version and ATA standard.
SMART Information	This page shows the results of the latest S.M.A.R.T test.
Test	Click on this tab to choose a rapid or complete S.M.A.R.T testing method for the hard disks. The test result will be shown.
Settings	Configure the following settings on this page: 1) Enable Temperature Alarm: enable this option to set the temperature alarm. When the hard disk temperature exceeds the specified threshold level, the system will record an error message; and 2) Rapid and complete test schedules: schedule a rapid or complete test here. The result of the latest test can be viewed on the "Summary" page. Click "APPLY to Selected HDD" to apply the settings configured on this page only to the selected hard disk drive or "APPLY to All HDDs" to all hard disk drives.

**Disk Health Global Settings**

You can enable the following Disk Health settings in the Global Setting dialog window (the "setting" icon next to "?" on top right side of the screen):

Activate Predictive SMART Migration: With Predictive SMART Migration, a warning message will pop up when an S.M.A.R.T error is detected on a hard disk drive (indicating that the RAID group that the hard drive disk belongs to is likely to fail very soon.) The migration sequence will be initiated for that RAID group to ensure the availability of that RAID group. The data from the disk with errors will be migrated to a healthy spare drive. The migration process is much faster than the standard rebuilding process.

Disk S.M.A.R.T polling time (minutes): This value is the interval the hard drive disks are scanned for S.M.A.R.T errors and the default is 10 minutes.

TLER/ERC timer (seconds): This option allows system administrators to configure the hard disk drive R/W response time. If you are not sure about the interval to set for the timer, please leave it as is.

## Managing Expansion Enclosures

First click an expansion enclosure (REXP) in the system component panel to check its general information. Refer to the following table for actions available to manage an expansion enclosure:

Action	Description
Enclosure Info	Click this button to check on details of the chosen enclosure, including the enclosure model, serial number, firmware version, BUS type, CPU temperature, system temperature, power status, system fan speed and power fan speed.
Locate (under "Action")	Click this button and the chassis LEDs of the selected expansion enclosure will blink for easy identification.
Safely Detach (under "Action")	Click this button to safely remove the enclosure from its host.
Update firmware (under "Action")	Click this button to update firmware for the chosen enclosure.
Rename enclosure (under "Action")	Click this button to rename the chosen enclosure.
RAID Group	Click this button and select a RAID group to check its details, including capacity, RAID group name, RAID type and disk member.

## Storage Space

The Storage Space features Storage Pools and Volumes. This page lists available storage pools and the volumes, and snapshots from remote QGW system on each of these storage pools. It displays these storage entities' capacity and/or usage to give a complete view of storage allocation. Users can create or manage storage pools/volumes/RAID groups, or take/view snapshots of the volumes on this page. For details on Storage Pools, Volumes, and RAID Groups, refer to the following links:

- [Storage Pools](#)
- [Volumes](#)
- [RAID Groups](#)

## Storage Pools

A storage pool is designed to aggregate physical hard disk drives into a large storage space and to provide enhanced RAID protection for it. You can perform the following actions to manage storage pools:

- [Creating New Storage Pools](#)
- [Removing Storage Pools](#)
- [Safely Detaching Storage Pools](#)
- [Expanding Storage Pools](#)
- [Setting a Threshold](#)
- [Setting Snapshot Reservation](#)
- [Creating New Volumes for Storage Pools](#)

## Creating New Storage Pools

Follow these steps to create a new storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Click "Create" > "New Storage Pool".
3. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk and click "Create".
4. Set the percentage of storage spool space that is reserved to store snapshots.
5. Please note that all data on the selected hard disk drive(s) will be erased. Click "OK" if you are certain about this.
6. A new storage pool will be created.

## Removing Storage Pools

Follow these steps to remove a storage pool:

- Go to "Storage Manager" > "STORAGE" > "Storage Space".
- Double click a storage pool to be removed to bring up the Storage Pool Management page.
- Click "Remove" > "Remove Pool".
- Click "Apply".
- The selected storage pool will be removed.

**Note:** Before you remove a storage pool, be sure to remove all volumes and LUNs on that storage pool.

## Safely Detaching Storage Pools

Follow these steps to safely detach a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be removed to bring up the Storage Pool Management page.
3. Click "Remove" > "Safely Detach Pool".
4. Click "Apply".
5. The selected storage pool will be removed.

## Expanding Storage Pools

Follow these steps to expand a storage pool:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.
3. Click "Expand Pool".
4. Select to create and add a new RAID group. Select "Adding new hard drive(s) to an existing RAID group"(the option "Create new RAID groups" will be covered in the following section), choose an existing RAID group from the drop-down list and click "Next".
5. Select the hard drive(s) to expand the storage pool and click "Next".
6. Click "Expand".
7. Please note that all data on the selected hard disk drive(s) will be erased. Click "OK" if you are certain about this.
8. The chosen storage pool will be expanded.

**Note:** Storage pool expansion is not supported for RAID 0 and RAID 1 configurations. For these configurations, it is necessary to create an additional RAID group in order to expand the storage pool.

## Expanding storage pools by creating new RAID groups

Follow these steps to create a RAID group for storage pool expansion:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.
3. Click "Expand Pool", select "Create and add a new RAID group" and click "Next".

4. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk and click "Next".
5. Please note that if the type of the newly-created RAID group is different from that of the existing RAID group(s), the performance of the entire storage pool may be affected. To continue, click "OK".
6. Click "Expand".
7. Please note that all data on the selected hard drive(s) will be erased. Click "OK" if you are certain about this.
8. The chosen storage pool will be expanded.

**Note:**

RAID 0 cannot be added to a storage pool if that storage pool already contains RAID 1. To expand storage space with an expansion unit, please create a separate static volume or storage pool on the expansion unit. A storage pool cannot be expanded using a USB-based expansion unit.

### Expanding storage pools by replacing hard disk drives in a RAID array

With this function, RAID group capacity can be expanded by replacing hard disk drives in an array one by one. This option is supported for RAID 1. Follow these steps to expand a RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to be expanded to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Expand Capacity".
4. Select at least one hard disk drive and click "Change". After the description displays "Please remove this drive", remove the hard disk drive from the QGW series or expansion enclosure.
5. After the description displays "You can replace this drive", plug in the new hard disk drive to the drive slot. Repeat the same process for all hard drives to be replaced. Click "Expand Capacity" to continue.
6. Click "Yes".
7. The chosen RAID group will be expanded.

**Note:** Available RAID management operations are detailed in the chapter on [RAID Groups](#).

### Setting a Threshold

The system will generate a warning message in system logs when the storage pool used size hits the threshold. To set a threshold value for a storage pool, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to set a threshold to bring up the Storage Pool Management page.
3. Click "Actions" > "Set Threshold".
4. Enter a value for alert threshold and click "Apply".

## Setting Snapshot Reservation

You can set snapshot reservation space to ensure enough space for saving snapshots. Snapshot reservation is set as a percentage of total storage pool space and there are two scenarios:

- When the snapshot reserve is set to 0%, new snapshots taken will all be saved to a storage pool until that storage pool runs out of its space. When that happens, the system will start recycling older snapshots regardless the snapshot limitation set in [Snapshot Global Settings](#).
- When the snapshot reserve is set to a value greater than 0%, this reserved space will be dedicated entirely to snapshots. The free space in a storage pool will be lower after the value is set and the snapshots will only use the space reserved. When the space used for snapshots exceeds the snapshot reserve, the system will start recycling older snapshots regardless the snapshot limitation set in [Snapshot Global Settings](#).

To set snapshot reservation, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to set reserved space for snapshots and to bring up the Storage Pool Management page.
3. Click "Actions" > "Set Snapshot Reserved", enter a value for snapshot reserved space, and click "Apply".

### Note:

For more Snapshot details, refer to the [Snapshot](#) section in the Volumes chapter.

Snapshots and related features are currently only available for the models with:

- \* A minimum of 4 GB RAM is required to use snapshots.
- \* Support up to 256 snapshots instead of 1024.

## Creating New Volumes for Storage Pools

To create a new volume for a storage pool, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool.
3. Click "Create"> "New Volume". Follow the onscreen instructions to finish the creation process. For more details, please refer to the [Volumes](#) section.

## Volumes

A volume is formatted by the file system to store share folders and files. Users can manage, monitor, create, or delete a logical volume on this page. The following topics are covered in this chapter:

- [Creating New Volumes](#)
- [Removing Volumes](#)
- [Expanding Volumes](#)
- [Available Volume operations](#)
- [Configuring Alert Threshold](#)
- [Creating New Shared Folders](#)
- [Snapshot](#)
- [Managing Previous Versions in Windows](#)
- [Encryption](#)
- [Setting Space Reclamation and SSD Trim](#)

## Creating New Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Click "Create" > "New Volume" to launch the volume creation wizard.
3. Configure the mode for the volume from static single, thick multiple, and thin multiple according to your needs (learn more about "Thick or Thin Volumes" in the following section) and click "Next".
4. Select the enclosure unit, hard disk drive(s), RAID type and hot spare disk for the volume to be created and click "Next".
5. Set the alert threshold and volume alias. You can also click "File system option" to specify bytes per inode, enable volume encryption and share folder creation. And click "Next".
6. Confirm your settings and click "Finish".
7. Please note that all data on the selected hard drive(s) will be erased. Click "OK" if you are certain about this.
8. The new volume will be created.

**Note:** The hot spare disk feature is only available for RAID 1. For other RAID types, the hot spare disk field will be grayed out.

Follow these steps to create a new, thick or thin volume:

1. Select "Thick Multiple Volume" or "Thin Multiple Volume". Select to create a new storage pool or from an existing storage pool and click "Next".
2. Configure the mode for the volume from static single, thick multiple, and thin multiple according to your needs.

3. Configure the volume capacity, alert threshold, volume alias, Bytes per inode, encryption and shared folder settings and click "Next".
4. Click "Finish".
5. A new volume will be created.

**Note:**

- **Static Single Volume:** This mode offers the best performance but does not support thin provisioning, space reclamation and snapshots. For this option, the RAID group itself is a volume.
- **Thick Multiple Volumes:** This method can create multiple volumes on the same storage pool and instantly allocate physical storage space for the volume. It has better performance than thin volumes while also offering flexibility.
- **Thin Multiple Volumes:** This method can over-allocate the volume capacity for each volume regardless of the physical storage limit, and the physical disk space is only used when files are written into the volume. After files are deleted, it is possible to reclaim the space with Space Reclaim and increase free space for storage pools. With thin provisioning, the volume space is fully utilized.
- A thick volume is usually more efficient for high frequency read/write activities. Because the space has been allocated for the volume, the predicament of insufficient physical space can be avoided, but the use of space is relatively inefficient.

## Removing Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to be removed to bring up the Volume Management page.
3. Click "Remove". Click "Apply" and the selected volume is removed.

## Expanding Volumes

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to be expanded to bring up the Volume Management page.
3. Click "Expand Volume".
4. Enter the desired capacity or click "Set to Max" to allocate the maximum available space for the volume and click "Apply". ("Set to Max" is only available for thick provisioned volumes.)
5. The capacity of the volume will be expanded.

## Available Volume Operations

After you go to "Storage Manager" > "STORAGE" > "Storage Space", click "Actions" and choose to configure the threshold and cache settings, check the file system of a volume, rename volume alias, reclaim volume space, create a new share folder, format a volume, or manage snapshots.

### Note:

- All the data on a disk will be erased if it is formatted. Please use the "Format" feature with caution.
- For encryption related options (Change, Download, Save, Lock this Volume), refer to [Encryption](#).
- It is recommended to format disk volumes larger than 2TB with EXT4.
- Snapshots and related features are currently only available for the following models.
  - \* A minimum of 4 GB RAM is required to use snapshots.
  - \* Support up to 256 snapshots instead of 1024.

## Configuring Alert Threshold

The alert threshold is used to remind users when the capacity of a chosen volume is used up to the specified threshold level. A warning message will pop up when the specified threshold is reached.

To set an alert threshold, select a volume in "Storage Space" to bring up the Volume Management page, click "Actions" > "Set Threshold", enter the threshold level and click "Apply". The alert threshold is set.

## Creating New Shared Folders

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a volume to bring up the Volume Management page.
3. Click "Actions" > "Create New Shared Folder".
4. Specify the folder name and description of the new shared folder and select the disk volume for the shared folder.
5. Click "Edit" to the right of "Configure access privileges for users" in Step 4 and specify user privileges.
6. Click "Edit" to the right of "Advanced settings" in Step 4 and configure the guest access right, hidden folder, Oplocks, recycle bin and path. Click "Create".
7. A new shared folder will be created.

## Snapshot

Users can take a snapshot, manage snapshots (revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files for LUNs or volumes), or replicate volumes/LUNs between different remote servers using snapshot technology.

### Note:

- Snapshot Replica (or volumes/LUNs replication between remote servers) is covered in Backup Station. For details, please refer to the Snapshot Replica chapter in Backup Station.
- Snapshots and related features are currently only available for the following models.
  - \* A minimum of 4 GB RAM is required to use snapshots.
  - \* Support up to 256 snapshots instead of 1024.

### Taking a Snapshot

After reserved space is set, you can proceed to take snapshots. To create a snapshot, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Select a volume or LUN and click "Snapshot" > "Take a Snapshot".
3. Specify the snapshot name and duration to retain the snapshot.
4. Click "OK".

### Managing Snapshots with Snapshot Manager

The Snapshot Manager allows you to take, revert, delete, and clone a snapshot, set up snapshot schedules, or restore snapshot files.

To launch Snapshot Manager, select a volume or LUN in "Storage Space" and click "Snapshot" > "Snapshot Manager" (or click the camera icon of a volume or LUN.)

In Snapshot Manager, you can perform the following actions:

- Restore files: Click a desired snapshot and select the folder(s) or file(s) that you want to restore, right click and select "Restore" to replace the existing folder/file with the one in the snapshot or "Restore to" to restore your data to a different location. Or choose "Download" to download the selection to your computer.
- Revert a snapshot: Select a snapshot and click "Revert", and the entire snapshot will be restored to its original path. Be cautious that the volume reverted to the selected snapshot will be in the previous state when the snapshot was taken.
- Delete: Select a snapshot and click "Delete" to delete that snapshot.
- Clone a snapshot: This action allows you to clone a snapshot into a new volume or LUN. To clone a snapshot, first select a snapshot, click "Clone", enter an alias for the new volume, and select the folders to share after cloning.

- Set up snapshot schedules: Click "Schedule", select "Enable schedule", specify the time, frequency, and retention period. The system will take the chosen volume's snapshot by schedule. For Smart Snapshot, the system will only take a new snapshot if there are new changes made in the selected volume.

### Snapshot Global Settings

Click "Global Settings" in the top-right of the Snapshot Manager window, and there is one global setting:

- Make snapshot directory (@Recently-Snapshot) visible: Mount a snapshot volume as a directory of a shared folder and set the snapshot volumes to be read-only in File Station. The snapshot directory will appear as "@Snapshot".

Click "Global Settings" in the top-right of the Storage Manager window, and there is one global setting:

- When reaching snapshot limitation: Choose the policy to handle snapshots when the snapshot limitation is reached. There are two choices.
  - Overwrite the oldest snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total) the oldest snapshot will be deleted in order to continue taking new snapshots for data protection.
  - Stop making snapshot: When the number of snapshots reaches the limitation (256 per LUN, 1024 total), no more new and scheduled snapshots will be taken until older snapshot are deleted. This option will prevent the deletion of older snapshots without administrators' consent.

**Note:** The "When reaching snapshot limitation" setting uses the number of snapshots, not the space used for snapshots. For more details, please refer to the [Setting Snapshot Reservation](#) section.

### Managing Previous Versions in Windows

Starting in QTS Gateway 4.2.1, snapshots can be used with the Previous Versions feature in Windows, allowing you to instantly revert to a previous version of a file in case of an accident (e.g. file deletion, corruption, or accidental changes.)

To use this feature, follow these steps:

1. [In Windows, connect to a shared folder on the QGW series](#) (the shared folder must be located in a storage pool that you can take a snapshot.)
2. Take a snapshot of the storage pool where the shared folder is located.
3. In Windows, right click on the shared folder (or a file in that shared folder) in "File Explorer" > "Properties" > "Previous Versions".

4. Select a version and choose to open, copy, or restore that version.
5. Click "OK".

**Note:** This feature is only applicable to files that have been changed between snapshots. Otherwise, there will be no previous versions listed in "File Explorer" > "Properties" > "Previous Versions".

## Encryption

The disk volumes on the QGW series can be encrypted with 256-bit AES encryption to protect against data breaches. Encrypted disk volumes can only be mounted for normal read/write access with an authorized password. The encryption feature protects confidential data from unauthorized access even if the hard drives or the entire QGW system were stolen.

**Note:** The AES volume-based encryption is applicable only to specific QGW models.

### Data encryption on QGW series

Users can manage encrypted disk volumes on the QGW series. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked using the following methods:

- Encryption password: Enter the encryption password to unlock the disk volume. The default password is "admin". The password must be 8-16 characters long. Symbols (! @ # \$ % ^ & \* ( ) \_ + = ? ") are supported.
- Encryption key file: Upload the encryption key file to the QGW series system to unlock the disk volume. The key can be downloaded from the "Encryption" page after the disk volume is successfully unlocked.

### Before you start

Please remember the following before using the data encryption feature of the QGW series.

- The volume encryption feature of the QGW series is volume-based. A volume can be a single disk or a RAID array. To only encrypt a shared folder, please refer to the Shared Folder chapter.
- Select whether or not to encrypt a disk volume before it is created on the QGW series. A volume cannot be encrypted after it is created unless the disk volume is initialized. Note that initializing a disk volume will clear all data on the disks.
- Disk volume encryption cannot be removed without initialization. To remove encryption on the disk volume, the disk volume must be initialized and all the data will be cleared.
- Keep the encryption password or key safe. If the password is forgotten or the encryption key is lost, the data cannot be accessed and cannot be recovered.

- Before starting, read the instructions carefully and strictly adhere to them.

**Note:** Data encryption functions may be unavailable in accordance to the legislative restrictions of some countries (ex. Russia, Belarus, Ukraine, Kazakhstan and Uzbekistan.)

### Creating new encrypted disk volumes

1. Log into the QGW series system as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space" and click "Create" > "New Volume".
2. Select a volume type based on your needs and click "Next".
3. Specify the volume details (including the volume capacity, alert threshold and volume alias,) tick "Encryption", fill out the encryption password and choose whether to save the encryption key, select to create a shared folder automatically after new volume initialization and fill out the name of the shared folder for the intended volume. Click "Next".
4. Confirm the settings and click "Finish".
5. Note that all the data on the selected drives will be DELETED! Please back up the data before creating the encrypted volume. Click "Yes" after data backup.
6. Double click the newly-created volume to bring up the Volume Management page.
7. Click "Actions" > "Encryption" > "Lock this Volume". Click "Yes".
8. An encrypted disk volume will be created on the QGW series.

### Encryption key management

To manage the encryption key settings, log into the QGW series as an administrator and go to "Storage Manager" > "STORAGE" > "Storage Space". Double click a volume to bring up the Volume Management page and click "Actions" > "Encryption".

There are three options to manage the encryption key:

- Change the encryption key: Enter your old encryption password and the new password. (Please note that after the password is changed, any previously exported keys will not work anymore. The new encryption key needs to be downloaded if necessary, see below.)
- Download the encryption key file: Enter the encryption password to download the encryption key file. With this option, the encryption key can be saved as a file. The file is also encrypted and can be used to unlock a volume, without knowing the real password (see "Locking and unlocking disk volumes manually" below.) Please save the encryption key file in a secure place!
- Save the encryption key: Save the encryption key on the QGW series to automatically unlock and mount the encrypted disk volume after the QGW system restarts. **Note that saving the encryption key alone is not completely safe, as if the QGW system is stolen, the volume will be automatically unlocked after it restarts.**

### Locking and unlocking disk volumes manually

To lock a volume, log into the QGW series as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". Double click a volume to be locked to bring up the Volume Management page and click "Actions" > "Encryption" > "Lock this Volume". Click "Yes".

To unlock a volume, log into the QGW series as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". Select a volume to be unlocked and click "Manage" > "Unlock this volume". Choose either to enter the encryption password, or use the encryption key file exported previously. Click "Apply". If the encryption password or the key file is correct, the volume will be unlocked and become available.

### Verifying encrypted disk volumes

To verify that a disk volume is encrypted, log into the QGW series as an administrator. Go to "Storage Manager" > "STORAGE" > "Storage Space". The encrypted disk volume will be shown on this page, with a lock icon under "Status". The lock will be shown as opened if the encrypted volume is unlocked. A disk volume without the lock icon under "Status" is not encrypted.

### Behaviors of encrypted volumes upon system reboot

An example is provided to illustrate the behavior of encrypted volumes upon system reboot. In this example, there are two encrypted disk volumes on the QGW series:

- DataVol1 is created with the option "Save Encryption Key" disabled.
- DataVol2 is created with the option "Save Encryption Key" enabled.

**Note:** For details on enabling or disabling the "Save Encryption Key" option, please refer to the section on Encryption Key Management above.

After restarting the QGW series system, check the volume status. DataVol1 is locked, but DataVol2 is unlocked and mounted. Since the encryption key is not saved on DataVol1, the encryption password needs to be manually entered to unlock DataVol1. Please remember that by saving the key on the QGW series, data will only be protected in case of stolen hard disk drives. However, there is still a risk of data breach if the entire QGW system is stolen as the data is accessible after the QGW system is restarted. If the encryption key is not saved on the QGW system, the QGW system will be protected against data breach even if the entire QGW system were stolen. The disadvantage is that the disk volume needs to be manually unlocked each time the system restarts.

## Setting Space Reclamation and SSD Trim

Space Reclamation allows you to reclaim space from deleted files to increase free space for storage pools, while SSD Trim enables the SSD to handle garbage collection overheads and improves future Write performance.

Click "Global Settings" (the "setting" icon next to "?" on the top-right side of the screen) to enable the function and its schedule. You will see two settings for Space Reclamation and SSD Trim:

- Auto reclaim and SSD trim schedule: the thin provisioning space reclamation will be started based on the schedule you set in order to reclaim space and increase free space for storage pools.
- Schedule: Set the Space and Reclamation and SSD Trim schedule.

## RAID Groups

Users can expand a RAID group, add hard drive(s) to a RAID group, configure a spare drive, enable a bitmap and recover a RAID group for a chosen volume, while the data contained in the RAID group remains intact. In this chapter, the following topics are covered:

- [RAID Group Introduction](#)
- [Expanding RAID Group Capacity](#)
- [Configuring Spare Drives](#)
- [Enabling/Disabling Bitmap](#)
- [Recovering Failed RAID Disk Volumes](#)

## RAID Group Introduction

### RAID group types

Refer to the table below for explanations on RAID types:

Field	Description
Single Disk	A single, stand-alone RAID group can be set up for your QGW series. However, this setup does not provide any redundancy protection. So, in the event that a disk is corrupted or otherwise damaged, all data on that disk will be lost.
RAID 0 Striping	A striping RAID group combines two or more disks into one large, logical disk. It offers the fastest disk access performance but no data redundancy protection in the event of disk failure or damage. The disk capacity is the sum of all disks. Disk striping is usually used to maximize disk capacity or to accelerate disk access speed. Please note that RAID 0 configuration is not recommended for storing sensitive data.
RAID 1 Mirroring	Disk Mirroring protects your data by automatically mirroring the contents of one disk to the second disk in the mirrored pair. It provides protection in the event of a single disk failure. The storage capacity is equal to the capacity of the smallest single disk, as the second disk drive is used to back up the first disk drive. RAID 1 configuration is suitable for storing sensitive data on a corporate or personal level.

## Expanding RAID Group Capacity

With this function, RAID group capacity can be expanded by replacing hard disk drives in a RAID group array one by one. This option is supported for RAID 1. Follow these steps to expand a RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Expand Capacity".
4. Select at least one hard disk drive. After the description displays "Please remove this drive", remove the hard disk drive from the QGW series or expansion enclosure.
5. After the description displays "You can replace this drive", plug in the new hard disk drive to the drive slot. Repeat the same process for all hard drives to be replaced. Click "Expand Capacity" to continue.
6. Click "Yes".
7. The chosen RAID group is expanded.

## Configuring Spare Drives

With this function, a spare drive can be added to or removed from a RAID 1 configuration. Follow these steps to configure a spare drive:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Configure Spare Drive".
4. Select the hard disk drive(s) to be configured as spare drive and click "Apply".
5. Please note that all data on the selected hard disk drive(s) will be erased. Click "Yes" if you are certain about this.
6. The chosen disk drives are added as spare drive.

## Enabling/Disabling Bitmap

This function can reduce the rebuild time after a crash, or the time length required to remove/re-add a hard disk. This feature does not improve disk read/write performance and may even cause slight performance degradation. However, if an array has a bitmap, a hard disk can be removed and re-added, and only changes in blocks need to be made since the removal (as recorded in the bitmap) can be re-synced. To enable a bitmap, follow these steps:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Enable Bitmap" and then "OK".

To disable a bitmap,

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a RAID group and click "Manage" > "Disable Bitmap" (only available after a bitmap has been enabled) and then "OK".

**Note:** Bitmap support is only available for RAID 1.

## Recovering Failed RAID Disk Volumes

This can recover failed RAID disk volumes from the "Inactive" status to a normal state (RAID 1 will be recovered to the degraded mode; RAID 0 will be recovered to the normal state.)

Before recovering a failed disk volume, please confirm that all hard disks of that disk volume are properly seated in the QGW system drive bays. Once recovery is completed, immediately back up your data on the disk(s) in case the disk volume fails again.

Inactive RAID disk volumes can only be recovered if the minimal number of healthy disks required for the RAID configuration is available on the QGW series. Refer to the following table for the minimal number of hard disks required to recover a RAID group:

RAID group	Minimal number of hard disks required for recovery
RAID 1	1

Follow these steps to recover a failed RAID group:

1. Go to "Storage Manager" > "STORAGE" > "Storage Space".
2. Double click a storage pool to bring up the Storage Pool Management page.
3. Select a failed RAID group.
4. Click "Manage" > "Recover".
5. The chosen RAID group will be recovered.

## Cache Acceleration

Based on SSD technology, the Cache Acceleration feature is designed to boost access performance of the QGW series. On this page, you can both monitor SSD performance and manage cache acceleration for your QGW series system. This chapter covers the following topics:

- [Feature Requirements](#)
- [Creating SSD Volumes](#)
- [Removing SSD Volumes](#)
- [Expanding SSD Volumes](#)
- [Configuring Volumes for SSD Cache](#)

### Feature Requirements

SSD drives must be installed to enable this function. Refer to the table below for memory requirements:

Cache Capacity	RAM Requirement *
512 GB	from 1 GB to 4 GB
1 TB	from 4 GB to 8 GB
2 TB	from 8 GB to 16 GB
4 TB	Above 16 GB

\*For example, for 1 TB of SSD capacity, at least 4GB RAMs are required for the QGW series.

On this page, users can choose to create, remove and expand a SSD volume and configure the SSD cache.

### Creating SSD Volumes

Follow the steps below to create a SSD volume:

1. Click "Create".
2. Select the SSD drive(s) and cache algorithm to create a SSD cache volume.
3. Select the cache type: Read-Only or Read/Write.
4. Click "Create".
5. Please note that all data on the selected hard drive(s) will be erased. Click "OK" if you are certain about this.
6. An SSD cache volume will be created.

**Note:** If SSD Cache is enabled with the Read-Write type, the SSD MUST NOT be removed while it is being used, as this will cause data loss.

## Removing SSD Volumes

Follow the steps below to remove a SSD volume:

1. Click "Remove".
2. Please note that all data on the selected hard drive(s) will be erased. Click "Yes" if you are certain about this.
3. The SSD volume will be removed. This operation can take a prolonged period if the SSD Cache is in Read/Write mode, as all the data in the cache must be flushed to the hard drive first.

## Expanding SSD Volumes

Follow the steps below to expand a SSD volume:

1. Click "Add SSD Drive".
2. Select the SSD drive(s) from the list and click "Expand".
3. Please note that all data on the selected hard drive(s) will be erased. Click "Yes" if you are certain about this.
4. The SSD volume will be expanded.

## Configuring Volumes for SSD Cache

Follow the steps below to configure volumes for a SSD cache:

1. Click "Cache Setting".
2. Select or deselect a volume to enable/disable the SSD cache, choose whether or not to record large block, sequential I/O operations in the cache space, and click "Finish".
3. The settings will be applied to the chosen volume.

### **Note:**

For larger block, sequential I/O operations such as video streaming, the hit rate is lower, and by default, they are not recorded in the cache space. If you need to record such operations, please cancel this setting, but please remember that after this setting is cancelled, more cache space and computing resources will be consumed for such operations.

Not all applications can benefit from a SSD cache. Please make sure that the SSD cache is supported by your applications.

## Snapshot Vault

Snapshot Vault stores snapshots created remotely from remote QGW series system via Snapshot Replica in Backup Station. It also lets you manage and restore remote snapshots.

### Note:

If this is the first time you use this feature, please configure [Snapshot Replica](#) in Backup Station on the source QGW series first.

Snapshots and related features are currently only available for the following models.

- \* A minimum of 4 GB RAM is required to use snapshots.
- \* Support up to 256 snapshots instead of 1024.

### Filtering Snapshots

Navigate to Snapshot Vault in Storage Manager and you will see a list of available snapshots. You can click the filter drop down list to filter snapshots with a set of criteria:

- Source: Source QGW system IP address
- Volume/LUN: The volume LUN that has been replicated
- Location: The storage pool where the snapshot has been stored
- Status: the snapshot status

**Note:** If the status of a snapshot is not "ready", you will not be able to view or access that snapshot.

### Displaying Snapshot Content

Navigate to Snapshot Vault in Storage Manager, choose the desired snapshot replication from the list, and click "Show Snapshots" to display the content of it. You can see synopsis of snapshots in the left panel or browse through folders and see files in the snapshots on the right panel.

Click "Hide snapshot content" next to the search box to review advanced information regarding snapshots in an expanded window.

To download files in a snapshot, select the files, right click your mouse and click "Download".

### Removing Snapshots

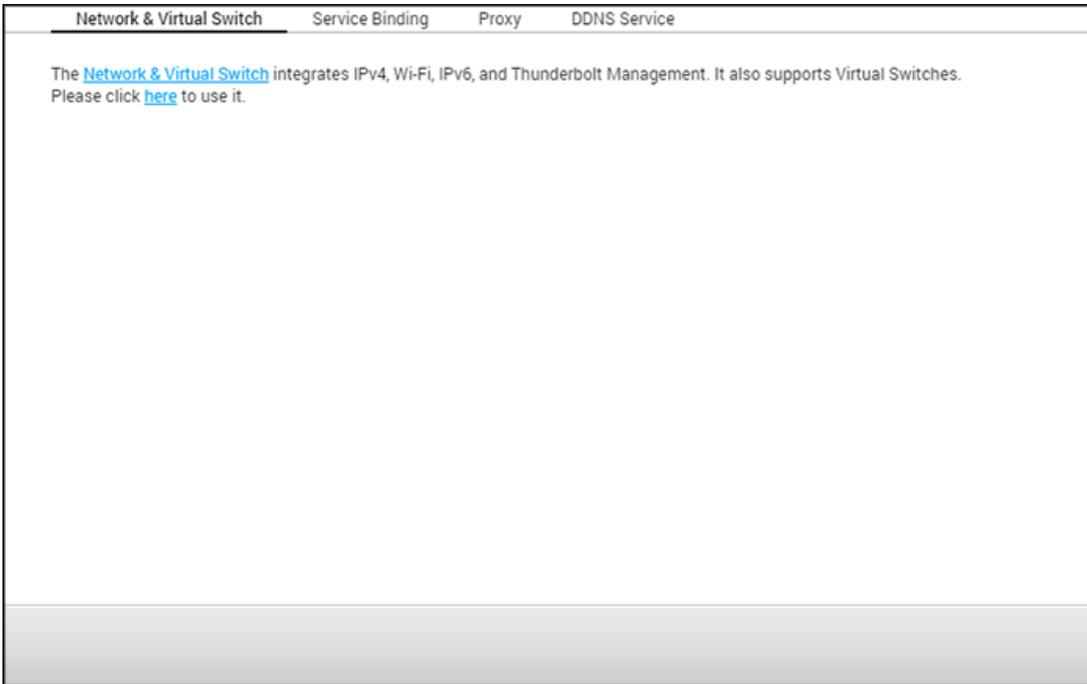
1. Navigate to Snapshot Vault in Storage Manager.
2. Select a snapshot replication in the list and click "Remove".
3. The snapshot replication is removed.

## Cloning Snapshots

1. Navigate to Snapshot Vault in Storage Manager.
2. Select a snapshot on the left panel and click "Clone".
3. Enter a name for the volume to mount the snapshot.
4. Choose the folders/files to clone.
5. Select "OK" and the task will start immediately.
6. Go to "Storage Manager" > "STORAGE" > "Storage Space" and you will see the new volume that has been cloned from Snapshot Vault.
7. You can now also use File Station to manage the files in the new volume.

# Network

Go to "Control Panel" > "System Settings" > "Network" to configure the QGW system network settings.



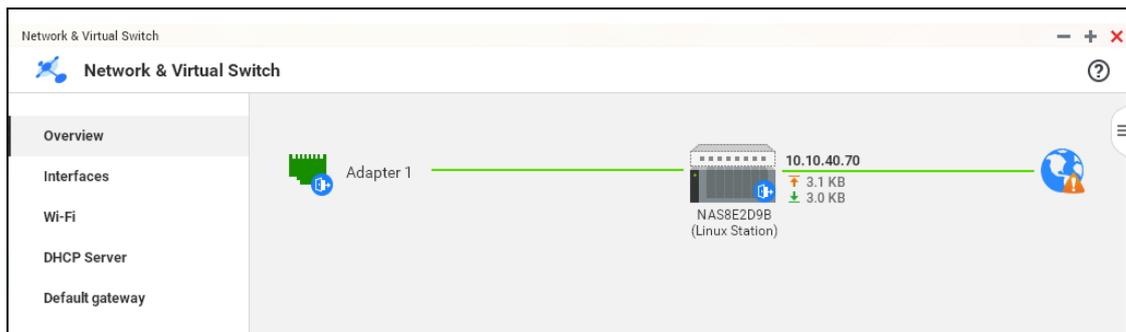
In this chapter, the following topics are covered:

- [Network & Virtual Switch](#)
  - [Overview](#)
  - [Interfaces](#)
    - [Physical interfaces](#)
      - [DNS Server](#)
      - [Port Trunking](#)
      - [IPv6](#)
    - [Virtual Switch](#)
  - [Wi-Fi](#)
  - [DHCP Server](#)
  - [Default Gateway](#)

## Network & Virtual Switch

The Network & Virtual Switch integrates physical interface management, Wi-Fi, DHCP server, default gateway, IPv6, and Thunderbolt management features. It also supports Virtual Switch. Virtual Switch can bridge 1 Gigabit and 10 Gigabit environments, just like using physical switches. You can bridge 1GbE devices and the QGW series via virtual switches, and also

bridge your QGW series and 10GbE environment for file access from the QGW series or remotely from the Internet.



## Overview

This page provides a general overview on the network and you can check the network topology, its status, each device on the network, downlink speed, uplink speed and the MAC address of each adaptor.

## Interfaces

You can edit physical interfaces, virtual switches, DNS server, port trunking and IPv6 settings on this page.

## Physical interfaces

Physical interfaces are LAN ports on the QGW series. To set physical interfaces, click the "interfaces" tab on the top of the page (next to "Virtual Switch"), select an adaptor from the list, and choose to configure its basic parameters, check their values, or refresh the list. After you click the "Configure" button next to an adaptor, you can edit the following values:

- IPv4:
  - Obtain the IP address settings automatically via DHCP: If the network supports DHCP, select this option and the QGW series will automatically obtain the IP address and network settings.
  - Use static IP address: To use a static IP address for network connections, select this option and enter the IP address, subnet mask, and default gateway. For the QGW series with two LAN ports, users can connect both network interfaces to two different switches and configure the TCP/IP settings. The QGW series will acquire two IP addresses which allow access from two different subnets. This is known as multi-IP settings\*. When using Qfinder to detect the QGW system IP, the IP of Ethernet 1 will be shown in LAN 1 only and the IP of Ethernet 2 will be shown in LAN 2 only. You can choose to use port trunking for a dual LAN connection.
  - Jumbo Frame: "Jumbo Frames" refers to Ethernet frames that are larger than 1500 bytes. It is designed to enhance Ethernet networking throughput and reduce the CPU utilization of large file transfers by enabling more efficient larger payloads per packet. The QGW series uses standard Ethernet frames (1500 bytes) by default. If network

appliances support Jumbo Frames, select the appropriate MTU value for the network environment. The QGW series supports 4074, 7418, and 9000 bytes for MTU.

**Note:**

- Jumbo Frame is only valid in Gigabit networks. All of the connected network appliances must enable Jumbo Frames and use the same MTU value.
  - Network Speed: Select the network transfer rate according to the network environment of the QGW series. Select auto negotiation and the QGW series will automatically adjust the transfer rate.
- VLAN: A Virtual LAN (VLAN) is a group of hosts which communicate as if they were attached to the same broadcast domain even if they are located in different physical locations. The QGW series can join a VLAN and be configured as a backup storage of other devices on the same VLAN. To join a VLAN, select "Enable VLAN (802.1Q)" and enter the VLAN ID (a value between 0 and 4094.) Keep the VLAN ID safe and make sure the client devices are able to join the VLAN. If you forget the VLAN ID and cannot connect to the QGW series, you will need to reset the network settings. Once the QGW series is reset, the VLAN feature will be disabled. If the QGW series supports two Gigabit LAN ports and only one network interface is configured to enable VLAN, you can also connect to the QGW series via the other network interface.

**DNS Server**

A DNS (Domain Name Service) server translates between a domain name (such as google.com) and an IP address (74.125.31.105.) On this page, you can configure the QGW series to obtain a DNS server address automatically or to specify the IP address of a DNS server. If you choose to specify the IP address, fill out the following fields:

- Primary DNS Server: Enter the IP address of the primary DNS server.
- Secondary DNS Server: Enter the IP address of the secondary DNS server.

**Note:**

- Contact your ISP or network administrator for the IP address of the primary and the secondary DNS servers. When the QGW series plays the role as a terminal and needs to perform independent connection enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
- If you obtain the IP address by DHCP, there is no need to configure the primary and secondary DNS servers. In this case, enter "0.0.0.0".

**Port Trunking**

The QGW series supports Port Trunking which combines two Ethernet interfaces into one to increase bandwidth and offers load balancing and fault tolerance (also known as failover.) Load balancing is a feature which distributes workloads evenly across two Ethernet interfaces for higher redundancy. Failover is the capability to maintain high availability by switching to a standby network interface ("slave" interface) when the primary network interface ("master" interface) does not correspond correctly.

To use Port Trunking on the QGW series, make sure at least two LAN ports of the QGW series have been connected to the same switch and the relevant settings (IP address, network speed, jumbo frame, VLAN, DHCP Server) have been configured.

Follow these steps to configure Port Trunking on the QGW series:

1. Click "Port Trunking".
2. Select the interfaces for a trunking group (adapter 1+2, adapter 3+4, adapter 5+6, or adapter 7+8.) Choose a Port Trunking mode from the drop-down menu. The default option is "Balance-rr" (Round-Robin). See the Port Trunking options table below for option details.
3. Select a Port Trunking group to use. Click "Apply".
4. Click "here" to connect to the login page.
5. Login to QTS Gateway.

**Note:**

- Make sure the Ethernet interfaces are connected to the correct switch and the switch has been configured to support the Port Trunking mode selected on the QGW series.
- Port Trunking is only available for QGW series models with two or more LAN ports.

The Port Trunking options available on the QGW series:

Field	Description	Switch Required
Balance-rr (Round-Robin)	Round-Robin mode is good for general purpose load balancing between two Ethernet interfaces. This mode transmits packets in sequential order from the first available slave through the last. Balance-rr provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
Active Backup	Active Backup only uses one Ethernet interface. It switches to the second Ethernet interface if the first Ethernet interface does not work properly. Only one interface in the bond is active. The bond's MAC address is only visible externally on one port (network adapter) to avoid confusing the	General switches

	switch. Active Backup mode provides fault tolerance.	
Balance XOR	Balance XOR balances traffic by splitting up outgoing packets between the Ethernet interfaces, using the same one for each specific destination when possible. It transmits based on the selected transmit hash policy. The default policy is a simple slave count operating on Layer 2 where the source MAC address is coupled with destination MAC address. Alternate transmit policies may be selected via the xmit_hash_policy option. Balance XOR mode provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
Broadcast	Broadcast sends traffic on both network interfaces. This mode provides fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
IEEE 802.3ad (Dynamic Link Aggregation)	Dynamic Link Aggregation uses a complex algorithm to aggregate adapters by speed and duplex settings. It utilizes all slaves in the active aggregator according to the 802.3ad specification. Dynamic Link Aggregation mode provides load balancing and fault tolerance but requires a switch that supports IEEE 802.3ad with LACP mode properly configured.	Supports 802.3ad LACP
Balance-tlb (Adaptive Transmit Load Balancing)	Balance-tlb uses channel bonding that does not require any special switch. The outgoing traffic is distributed according to the current load on each Ethernet interface (computed relative to the speed.) Incoming traffic is received by the current Ethernet interface. If the receiving Ethernet interface fails, the other slave takes over the MAC address of the failed receiving slave. Balance-tlb mode provides load balancing and fault tolerance.	General switches

Balance-alb (Adaptive Load Balancing)	Balance-alb is similar to balance-tlb but also attempts to redistribute incoming (receive load balancing) for IPV4 traffic. This setup does not require any special switch support or configuration. The receive load balancing is achieved by ARP negotiation sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the Ethernet interfaces in the bond such that different peers use different hardware address for the server. This mode provides load balancing and fault tolerance.	General switches
--	--	------------------

To delete a Port Trunking group, first select a group from the list and click "Delete".

To be automatically notified if a network cable has been disconnected, check "Warn me if a network cable is disconnected from the trunking group" on this page.

## IPv6

The QGW series supports IPv6 connectivity with "stateless" address configurations and RADVD (Router Advertisement Daemon) for IPv6, RFC 2461 to allow the hosts on the same subnet to automatically acquire IPv6 addresses from the QGW series. QGW series services which support IPv6 include:

- CIFS/SMB
- AFP
- NFS
- FTP
- Web Server
- QTS Gateway Desktop
- RTRR
- SSH
- Qsync for Windows
- Netbak Replicator

To use this function, select the option "Enable IPv6" and click "Apply". The QGW series will restart. After the system restarts, go to the IPv6 page. The settings of the IPv6 interface will be shown. Click the "Edit" button to edit the settings:

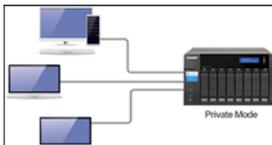
- **IPv6 Auto** Configuration: If an IPv6 enabled router is available on the network, select this option to allow the QGW series to automatically acquire the IPv6 address and configurations.

- **Use static IP address:** To use a static IP address, enter the IP address (e.g. 2001:bc95:1234:5678), prefix length (e.g. 64), and the gateway address for the QGW series. Contact your ISP for the prefix and the prefix length information.
  - **Enable Router Advertisement Daemon (radvd):** To configure the QGW series as an IPv6 host and distribute IPv6 addresses to the local clients which support IPv6, enable this option and enter the prefix and prefix length.
- **IPv6 DNS server:** Enter the preferred DNS server in the upper field and the alternate DNS server in the lower field. Contact the ISP or network administrator for the information. If IPv6 auto configuration is selected, leave the fields as "::".

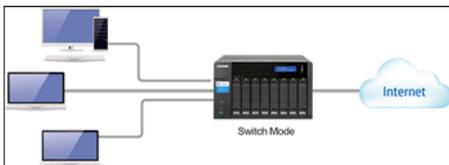
## Virtual Switch

With this feature, you can choose to set up a private network with your QGW series (Private Network mode) or set the QGW series as a switch (Switch mode) for all the connected devices.

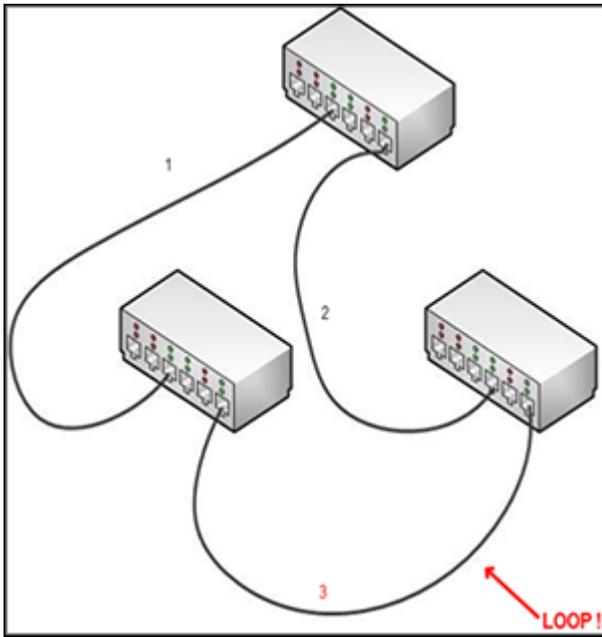
- **Private Network mode:** You can specify network ports on the QGW series and distribute IP addresses to devices in the downlink for the creation of a private network.



- **Switch mode:** You can configure adapters to uplink/downlink between QGW system and devices. After setting this option, devices and QGW system can share the network to each other.



As you connect your devices for each of the modes, please be extra cautious and make sure that selected interfaces are not within the same LAN environment. Otherwise, it will generate a network loop that may crash your network environment.



To add a virtual switch and set Private Network mode, click "Add" > "Private Network Mode" and select the adapters and DHCP server settings (The start IP address, end IP address and lease time.) Click "More Settings" to add the WINS server, DNS suffix, TFTP server and Boot file settings. Click "Add" after you finish adding all the settings.

To add a virtual switch and set Switch mode, click "Add" > "Switch Mode" and select the adapters and specify their type (downlink interface (could be multiple interfaces) or uplink interface (only one)) and click "Add".

To edit a virtual switch, click the "edit" icon next to a virtual switch. To delete a virtual switch, first select a virtual switch from the list and click "Delete".

**Tip:** You can click ">" next to an adapter or virtual switch to check its status and details.

## Wi-Fi

To connect to a Wi-Fi network, plug a USB Wi-Fi dongle into the QGW series, and a list of Wi-Fi access points will be shown. There are two ways to connect to Wi-Fi networks:

- Connecting to an existing Wi-Fi network.
- Manually connecting to a Wi-Fi network.

**Note:** Wireless connection performance depends on many factors such as the adapter model, the USB adapter's performance, and the network environment. Wired connections will always provide greater stability and performance.

### Method 1: Connecting to an existing Wi-Fi network:

A list of Wi-Fi access points with signal strength are displayed in "Wi-Fi Network Connection".

Icon / Option	Name	Description
Rescan	Rescan	Search for Wi-Fi networks in range.
	Secured network	The Wi-Fi network requires a network key.
	Connect	Connect to a Wi-Fi network. If a security key is required, you will be prompted to enter the key.
	Edit	Edit the connection information. You can select to automatically connect to the Wi-Fi network.
	Disconnect	Disconnect from the Wi-Fi network.
	Remove	Delete the Wi-Fi network profile.
Show all	Show all	Display all available Wi-Fi networks. Deselect this option to only show configured network profiles.

Click "Rescan" to search for available Wi-Fi networks. Select a Wi-Fi network to connect to and click "Connect". Enter the security key if needed. Click "Next" and the QGW series will attempt to connect to the wireless network. You can view the status of the configured network profiles.

Message	Description
Connected	The QGW series is currently connected to the Wi-Fi network.
Connecting	The QGW series 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 broadcast.
Failed to get IP	The QGW series 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 QGW series cannot connect to the Wi-Fi network. Check the router settings.
Incorrect key	The entered security key is incorrect.
Auto connect	Automatically connect to the Wi-Fi network. This is not supported if the SSID of the Wi-Fi network is not broadcast.

## Method 2: Manually connecting to a Wi-Fi network:

To manually connect to a Wi-Fi network that does not broadcast its SSID (network name), click "Connect to a Wi-Fi network".

You can choose to connect to an ad hoc network in which you can connect to any wireless devices without the need for an access point. To set up, follow these steps:

1. Enter the network name (SSID) of the wireless network and select the security type.
  - o No authentication (Open): No security key required.
  - o WEP: Enter up to 4 WEP keys and choose 1 key to be used for authentication.
  - o WPA-Personal: Choose AES or TKIP encryption and enter the encryption key.
  - o WPA2-Personal: Enter a security key.
2. Type in the security key.
3. Click "Finish" after the QGW series has added the Wi-Fi network.
4. To edit IP address settings, click "Edit". You can choose to automatically obtain the IP address by DHCP or to set a fixed IP address.

If the Wi-Fi connection is the only connection between the QGW series and the router/AP, you must select "WLAN1" as the default gateway in "Network" > "TCP/IP" page. Otherwise, the QGW series will be unable to connect to the Internet or communicate with another network.

### Note:

- The WEP key must be exactly 5 or 13 ASCII characters; or exactly 10 or 26 hexadecimal characters (0-9 and A-F.)
- If you have trouble connecting to an encrypted wireless network, check the wireless router/AP settings and change the transfer rate from "N-only" mode to "B/G/N mixed" or similar settings.
- Windows 7 users with WPA2 encryption cannot establish ad-hoc connection with the QGW series. WEP encryption must be used on Windows 7.
- A fixed IP address is required for wireless interfaces to establish an ad-hoc connection.

## DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to clients on a network. Select "Enable DHCP Server" to set the QGW series a DHCP server if there are none on the local network where the QGW series is located.

### Note:

- Do not enable DHCP server if there is one on the local network to avoid IP address conflicts or network access errors.

- The DHCP server option is only available to Ethernet 1 when both LAN ports of a QGW system are connected to the network and configured as standalone IP settings.
- **Start IP, End IP, Lease Time:** Set the range of IP addresses allocated by the QGW series to the DHCP clients and the lease time. The lease time refers to the time that an IP address is leased to the clients. During that time, the IP will be reserved to the assigned client. When the lease time expires, the IP can be assigned to another client.
- **WINS Server (optional):** WINS (Windows Internet Naming Service) resolves Windows network computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. Enter the IP address of the WINS server on the network if available.
- **DNS Suffix (optional):** The DNS suffix is used for resolution of unqualified/incomplete host names.
- **TFTP Server & Boot File (optional):** The QGW series supports PXE booting of network devices. Enter the IP address of the TFTP server and the boot file (including directory on the TFTP server and file name.) For remote booting of devices, enter the public IP address of the TFTP server.

### Default Gateway

Select the gateway settings to use if both LAN ports have been connected to the network (dual LAN models only.)

# Security

Go to "Control Panel" > "System Settings" > "Security" to configure relevant security settings for your QGW series.

The screenshot shows the "Security Level" configuration page. At the top, there are three tabs: "Security Level" (selected), "Network Access Protection", and "Certificate & Private Key". Below the tabs, there are three radio button options: "Allow all connections", "Deny connections from the list" (which is selected), and "Allow connections from the list only". A horizontal line separates this section from the next. Below the line, there is a text prompt: "Enter the IP address or network from which the connections to this server will be allowed or rejected." Underneath this prompt are two buttons: "Add" and "Remove". Below these buttons is a table with three columns: "Genre", "IP Address or Network Domain", and "Time Left for IP Blocking". The table is currently empty. At the bottom of the page, there are two buttons: "Apply" and "Apply All".

## Security Level

Specify the IP address or network domain from which connections to the QGW series are allowed or denied. When the connection of a host server is denied, all the protocols of that server are not allowed to connect to the QGW series. After changing the settings, click "Apply" to save the changes. Network services will be restarted and current connections to the QGW series will be terminated.

## Network Access Protection

Network access protection enhances system security and prevents unwanted intrusion. You can block an IP for a certain period of time or indefinitely if the IP fails to login to the QGW series system from a particular connection method.

## Certificate & Private Key

Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload an SSL certificate issued by trusted providers. After uploading an SSL certificate, users can connect to the administration

interface of the QGW series by SSL and there will not be any alert or error message. The QGW series only supports X.509 certificates and private keys.

- Download Certificate: Download the secure certificate which is currently in use.
- Download Private Key: Download the private key which is currently in use.
- Restore Default Certificate & Private Key: Restores the secure certificate and private key to system default. The secure certificate and private key in use will be overwritten.

# Hardware

Go to "Control Panel" > "System Settings" > "Hardware" to configure the QGW system hardware functions.

The screenshot shows the 'Hardware' configuration page with the 'General' tab active. It contains the following settings:

- Enable configuration reset switch
- Enables hard disk standby mode: The status LED will turn off if there is no access within  
Time: 30 minutes
- Enables the light signal alert when the free storage size is less than the value  
Size: 3072 MB
- Enable write cache (EXT4 delay allocation)

An 'Apply All' button is located at the bottom of the configuration area.

## General

- **Enable configuration reset switch:**
  - **Basic system reset:** After pressing and holding the reset button for 3 seconds, the following settings will be reset to default:
    - System administration password: admin.
    - TCP/IP configuration: Obtain IP address settings automatically via DHCP.
    - TCP/IP configuration: Disables Jumbo Frames.
    - TCP/IP configuration: If port trunking is enabled, the port trunking mode will be reset to "Active Backup (Failover)".
    - System port: 8080 (system service port.)
    - Security level: Low (Allows all connections.)
    - VLAN will be disabled.
    - Service binding: All QGW services will be run on all available network interfaces.
- **Enable hard disk standby mode:** This option allows the QGW system drives to enter standby mode if there is no disk access within the specified period.
- **Enable write cache (EXT4 only):** If the QGW system disk volume uses EXT4, enable this option for higher write performance. Note that an unexpected system shutdown may lead to data loss. This option will be disabled if the following services are enabled: Download Station, MySQL service, user quota, and Surveillance Station. It is

recommended to disable this option if the QGW series is set as shared storage in a virtualized or clustered environment.

- **Enable warning alert for redundant power supply on the web-based interface:** If two power supply units (PSU) are installed on the QGW series and connected to the power sockets, both PSU will supply the power to the QGW series (applied to 1U and 2U models.) Turn on the redundant power supply mode in "System Settings" > "Hardware" to receive warnings for the redundant power supply. The QGW series will sound and record error messages in "System Logs" if the PSU is plugged out or does not respond correctly. If only one PSU is installed on the QGW series, DO NOT enable this option. This function is disabled by default.

## **Buzzer**

**Enable alarm buzzer:** Enable this option to allow the alarm buzzer to beep when certain system operations (startup, shutdown, or firmware upgrade) are executed.

## **Write Cache**

Better write performance can be obtained when this option is enabled. Please note that an unexpected system shutdown may cause data loss. This option is disabled when the Download Station or SQL service is enabled.

# Power

You can restart or shut down the QGW series, specify the behavior of the QGW series after a power recovery, and set the schedule for automatic system power on/off/restart on this page.

Power Schedule

Enable schedule

Postpone the restart/shutdown schedule when a replication job is in progress.

Add Remove

Action	Schedule Type	Hour	Minute
Shutdown	Daily	7	0

Apply All

## EuP Mode Configuration

EuP (also Energy-using Products) is a European Union (EU) directive designed to improve the energy efficiency of electrical devices, reduce the use of hazardous substances, increase ease of product recycling, and to improve environment-friendliness of products.

When EuP is enabled, the following settings will be affected so that the QGW series maintains low power consumption (less than 1W) when the QGW series system is powered off:

- Wake on LAN: Disabled.
- AC power resumption: The QGW series will remain off after the power restores from an outage.
- Scheduled power on, off, restart settings: Disabled.

When EuP is disabled, the power consumption of the QGW series is slightly higher than 1W when the QGW series is powered off. EuP is disabled by default so that you can use the functions Wake on LAN, AC power resumption, and power schedule settings properly.

## Power Schedule

Specify the schedule for automatic system power on/off, restart, or sleep mode. Weekdays are Monday to Friday, weekends are Saturday and Sunday. Up to 15 schedules can be set.

Enable "Postpone the sleep/restart/shutdown schedule when replication job is in process" to allow scheduled system restart/shutdown to be carried out after a running replication job completes. Otherwise, the QGW series will ignore the running replication job and execute scheduled system restart or shutdown.

### Note:

- The system cannot be shut down or restarted in sleep mode.
- If there are other QNAP storage expansion enclosures connected to the QGW series, the sleep mode will be disabled automatically and system will not go into sleep mode.

# Notification

Go to "Control Panel" > "System Settings" > "Notification" to configure notifications.

The screenshot shows a web interface for configuring notifications. At the top, there are three tabs: "E-mail", "SMS", and "Push Service". The "E-mail" tab is selected. Below the tabs, there are two main sections: "SMTP Server" and "Alert Notification".

**SMTP Server**

Select an e-mail account:

SMTP server:

Port number:

E-mail:

Username:

Password:

Secure connection:

**Alert Notification**

When the following system events occur:

At the bottom of the form, there is a button labeled "Apply All".

## E-mail

The QGW series supports email alerts to inform the administrator of system errors and warnings. To receive alerts by email, configure the SMTP server.

- Select an email account: specify the type of email account you would like to use for email alerts.
- SMTP Server: Enter the SMTP server name (for example: smtp.gmail.com.)
- Port Number: Enter the port number for the SMTP server. The default port number is 25.
- E-mail: Enter the email address of the alert recipient.
- Username and Password: Enter the email account's login information.
- Secure connection: Choose SSL or TLS to ensure a secure connection between the QGW series and SMTP server or None. It is recommended to use this if the SMTP server supports it.
- Alert Notification: Select the type of instant alerts the QGW series will send when system events (warnings/errors) occur. A maximum of two email addresses can be specified to receive alerts from the QGW series.

## SMS

Configure the SMSC server settings to send SMS messages to specified phone numbers from the QGW series. Follow these steps to set up a SMSC server:

1. Choose an SMS service provider. The default SMS service provider is Clickatell. You can add your own SMS service provider by selecting "Add SMS Provider" from the drop-down menu. When "Add SMS service provider" is selected, enter the name of the SMS provider and the URL template text.
2. Specify to enable SSL connection to the SMS service provider and fill out the server details, including the login name, login password and server API\_ID.
3. Enable the alert notification by ticking the checkbox "When a system error event occurs, send a SMS notification to the following phone number". Up to two phone numbers can be specified to receive instant system alerts from the QGW series.

**Note:** The URL template text must follow the standard of the SMS service provider to receive the SMS alert properly.

## Push Service

The push service lets you receive notification messages on your mobile devices if a warning or error event occurs - allowing you to quickly receive first-hand information from your QGW series and instantly react to keep your data safe. You must have "Qmanager" installed on your mobile devices to receive notifications.

**Note:** You must have firmware QTS Gateway 4.2.0 with Qmanager iOS 1.8.0 / Qmanager Android 2.1.0 or above.

Follow these steps to set up the push service:

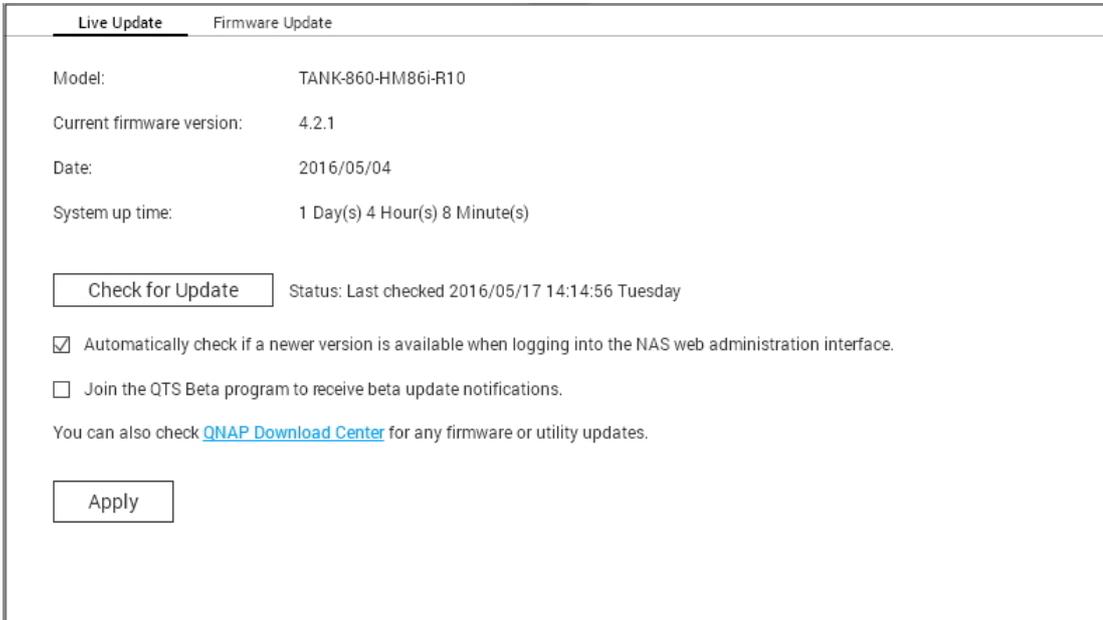
1. Log into myQNAPcloud using your QID.
2. Choose the notification types that you want to receive (warnings or errors.)
3. Install Qmanager on your mobile device (Qmanager iOS 1.8.0 / Android 2.1.0 or above.)
4. Log into the QGW series using Qmanager and confirm to receive push notifications (you can also disable this service in Qmanager > click ">" next to a QGW connection > "server settings" page > change push service properties.)
5. The QGW series will send alert notifications to paired mobile devices when a warning or error event occurs.

The paired devices will be listed in the "Manage Paired Devices" table. You can disable or delete a paired device from the table.

**Note:** On occasion you may not receive system notifications instantly due to iOS and Android server mechanisms.

# Firmware Update

Go to "Control Panel" > "System Settings" > "Firmware Update" to update the firmware version of the QGW series. Note: The following screenshot is captured from a TANK-860 system. The exact model name may vary across the various QGW series systems.



The screenshot shows the "Firmware Update" page with the following information:

Live Update	Firmware Update
Model:	TANK-860-HM86i-R10
Current firmware version:	4.2.1
Date:	2016/05/04
System up time:	1 Day(s) 4 Hour(s) 8 Minute(s)

Status: Last checked 2016/05/17 14:14:56 Tuesday

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.

You can also check [QNAP Download Center](#) for any firmware or utility updates.

## Live Update

Select "Automatically check if a newer version is available when logging into the web administration interface" to allow the QGW series to automatically check if a new firmware version is available. If a new firmware is found, you will be notified after logging in the QGW series as an administrator. Click "Check for Update" to check if any firmware update is available. Note that the QGW series must be connected to the Internet for these features to work.

## Firmware Update

Before updating the system firmware, make sure the product model and firmware version are correct. Follow these steps to update the firmware:

1. Download the firmware release notes from the IEI website. Read the release notes carefully to make sure it is necessary to update the firmware.
2. Download the firmware and unzip the IMG file to the computer.
3. Before updating the system firmware, back up all the QGW system data to avoid any potential data loss from unforeseen issues arising during the system update.
4. Click "Browse" to select the firmware image for the system update. Click "Update System" to update the firmware.

The system update may take seconds, minutes or longer to complete depending on the network connection status. The QGW series will inform you when the system update has completed.

**Note:**

- If the system is running properly, you do not need to update the firmware.
- QTS Gateway does not support downgrading the firmware. However, if you choose to apply an older firmware version, please back up all of your important data before downgrading. IEI is not responsible for any damage to the QGW series or its contents after downgrading.

### **Update Firmware by Qfinder Pro**

The firmware can be updated using Qfinder Pro by following these steps:

1. Select a QGW series model and choose "Update Firmware" from the "Tools" menu.
2. Login to the QGW series as an administrator.
3. Browse and select the firmware for the QGW series. Click "Start" to update the system.

**Note:** If you have multiple identical QGW system on the same LAN, they can be updated at the same time with Qfinder Pro. Administrator access is required.

# Backup/Restore

Go to "Control Panel" > "System Settings" > "Backup/Restore" to back up, restore your QGW series or restore your QGW series to factory default settings.

The screenshot shows a web interface for Backup/Restore Settings. At the top, there are two tabs: "Backup/Restore Settings" (which is active) and "Restore to Factory Default". Below the tabs, the "Back up System Settings" section contains a "Backup" button. The "Restore System Settings" section contains a "Browse..." button and a "Restore" button. The interface is clean and uses a light gray color scheme.

## Backup/Restore Settings

- **Back up System Settings:** To back up all the settings, including the user accounts, server name, network configuration and so on, click "Backup" and select to open or save the setting file. Settings will be backed up include: User, Group, Shared Folder, Workgroup, Domain, and LDAP, Windows File Service, Mac File Service, NFS, FTP, WebDAV, Network Backup, User Home, Password Settings, SNMP, and Backup Service.
- **Restore System Settings:** To restore all the settings, click "Browse" to select a previously saved setting file and click "Restore".

### Note:

- User Home includes basic service settings (excluding user data in the user home folder.)
- If the users or groups you try to restore from the backup file already exist in the current system, the users and groups in the current system will be overwritten.

## Restore to Factory Default

- **Restore Factory Defaults & Format all Volumes:** Restore system settings to default and **formats all disk volumes**.
- **Reset Settings:** Restore system settings to default without erasing user data.
- **Reinitialize NAS:** **Erases all data** and reinitializes the NAS.

**Caution:** The administrator's password and system settings will be reset to default if you press and hold the clear CMOS button inside the QGW series for 3 seconds (data and files on the QGW series will be unaffected.)

# External Device

Go to "Control Panel" > "System Settings" > "External Storage" to configure external storage devices, USB printers and UPS systems.



For details on these features, refer to the following links:

- [External Storage](#)
- [USB Printer](#)
- [UPS](#)

# External Storage

The QGW series supports USB storage devices for backup and data storage. Connect the external storage device to a USB port of the QGW series and its details will be shown on this page.

In this chapter, the following topics are covered:

- [Storage Information](#)
- [Format](#)
- [Eject](#)
- [Encryption Management](#)
- [Data Sharing](#)

## Storage Information

Select a storage device and click "Storage Information" to check its details. The number of USB interfaces supported varies by model. It may take a few seconds for the QGW series to detect external USB devices.

## Format

External storage devices can be formatted as EXT3, EXT4, FAT32, NTFS, or HFS+ (Mac only). Click "Format" and select the option from the drop-down menu.

The QGW series supports encrypting external drives. To encrypt an external storage device, click "Encryption". Select the encryption method: AES 128-, 192- or 256-bit and enter the password (8-16 characters.) Select "Save encryption key" to save the password in a hidden location on a hard drive in the QGW series. The QGW series will automatically unlock the encrypted external storage device when the device is connected. Click Format to proceed. Click "OK" and all the data will be cleared. The device will be "Ready" after disk initialization.

**Note:** We recommend formatting disk volumes larger than 2TB using EXT4, NTFS, or HFS+.

## Eject

"Eject" offers two different options. "Disconnect disk partition" allows you to remove a single disk partition or a disk drive in a multi-drive enclosure. "Remove device" allows you to disconnect external storage devices without the risk of losing any data when the device is

removed. First choose a device to eject, click "Eject" and then disconnect the disk partition or remove the device.

**Note:** To avoid potential data loss, always use the hardware removal function before removing your external storage device (for a Windows PC, use the "Safely Remove Hardware"; for a Mac, use the "Eject" icon; for QTS Gateway, use the "Eject" button.)

## Encryption Management

If an external storage device is encrypted by the QGW series, the button "Encryption Management" will appear. Click this button to manage the encryption password/key, or to lock/unlock the device.

### Locking the device

1. To lock an encrypted external storage device, click "Encryption Management".
2. Select "Lock this device" and click "Next".
3. Click "Next" to lock the device.

**Note:** External storage devices cannot be locked if a real-time or scheduled backup job is running on it. To disable the backup job, go to "Control Panel" > "Applications" > "Backup Station" > "External Drive".

### Unlocking the device

1. To unlock an encrypted external storage device, click "Encryption Management".
2. Select "Unlock this device". Click "Next".
3. Enter the encryption password or upload the key file. Select "Save encryption key" to save the password in a hidden location on a hard drive of the QGW series. The QGW series will automatically unlock the encrypted external storage device every time the device is connected.

### Managing the encryption key

1. To change the encryption password or download an encryption key file, click "Encryption Management".
2. Select "Manage encryption key". Click "Next".
3. Select to change the encryption password or download the encryption key file to the local PC.

## Data Sharing

Select "Data sharing" for an external storage device connected to the QGW series.

**Note:** HD Station will reboot when external devices are unmounted.

## USB Printer

The QGW series supports network printing sharing service over local networks and the Internet in Windows, Mac, and Linux (Ubuntu) environments. Up to 3 USB printers are supported.

To share a USB printer, connect the printer to a USB port on the QGW series. The printer will be automatically detected and its information displayed.

### Printer Info

Click on a connected USB printer and then "Printer Info" to review its details.

#### Note:

- Connect a USB printer to the QGW series after the software configuration is completed.
- The QGW series does not support multifunction printers.
- The file name display for the printer job table is only available for printer jobs sent via IPP (Internet Printing Protocol).

### Printer Log

Click on a connected USB printer and then "Printer Log" to view its print job history. You can pause or cancel ongoing/pending jobs, resume paused jobs, or delete completed or pending jobs. To clear the history, click "Clear".

**Note:** Do NOT restart the QGW series or update the system firmware when printing is in process or there are queued jobs. Otherwise all the queued jobs will be cancelled and removed.

### Clean Up Spool Space

Click "Clean Up Spool Space" to clean up the data saved in the printer spool.

### Settings

Click "Settings" to configure basic settings of the printer.

- **Stop printer sharing and clear print spool:** Select this option to temporarily disable the selected printer for print sharing. All of the data in the printer spool will be cleared.

- **Bonjour printer support:** Select this option to broadcast printing service to Mac users via Bonjour. When naming your printer, the name can only contain "a-z", "A-Z", "0-9", dot (.), comma (,) and dash (-).

#### **Maximum Printer Jobs and Blacklist**

- **Maximum printer jobs per printer:** Specify the maximum number of printer jobs for a printer. A printer supports up to 1,000 printer jobs. The oldest printer job will be overwritten by the newest one if the printer has reached the maximum number of printer jobs.
- **Enter IP addresses or domain names to allow or deny printing access:** To allow or deny particular IP addresses or domain names from using the printing service, select "Allow printing" or "Deny printing" and enter the IP addresses or domain names. An asterisk (\*) denotes all connections. To allow all users to use the printer, select "No limit". Click "Apply" to save the settings.

**Note:** This feature only works for printing service via IPP and Bonjour, but not Samba.

## Windows 7

Follow these steps to set up your printer connection:

1. Go to Devices and Printers.
2. Click "Add a printer".
3. In the Add printer wizard, click "Add a network, wireless or Bluetooth printer".
4. While Windows is searching for available network printers, click "The printer that I want isn't listed".
5. Click "Select a shared printer by name", and then enter the address of the network printer. The address is in the following format –  
`http://QGW_IP:631/printers/ServernamePR`, where the QGW\_IP can also be a domain name address if you want to print remotely. For example,  
<http://10.8.13.59:631/printers/NASPR3>
6. The wizard will prompt you for the correct printer driver. You can also download the latest printer driver from the manufacturer's website if it is not built-into Windows operating system.
7. After installing the correct printer driver, the wizard shows the address and driver of the new network printer.
8. You can also set the network printer as the default printer or print a test page. Click "Finish" to exit the wizard.
9. The new network printer is now available for printing.

## Mac OS 10.6

If you are using Mac OS 10.6, follow these steps to configure the printer function:

1. First make sure that Bonjour is enabled on the QGW series in "External Device" > "USB Printer" > "Settings". You can change the Service Name to better represent the printer.
2. On your Mac, go to "System Preferences", and then click "Print & Fax".
3. In the Print & Fax window, click + to add a printer.
4. The USB network printer will be listed via Bonjour. Select the default printer driver or download and install the latest one from the printer manufacturer's website. Click "Add" to add this printer.
5. Additional options may be available for your printer. Click "Continue".
6. The new network printer is now available for printing.

## Mac OS 10.5

If you are using Mac OS X 10.5, follow these steps to configure the printer function:

1. Go to "Network Services" > "Win/Mac/MFS" > "Microsoft Networking". Enter a workgroup name for the QGW series. You will need this information later.
2. Go to "Print & Fax" on your Mac.
3. Click + to add a printer.
4. Select the QGW series workgroup and find the printer name.
5. Enter the username and password to login the printer server on the QGW series.
6. Select the printer driver.
7. After installing the printer driver correctly, you can start using the printer.

## Mac OS 10.4

If you are using Mac OS 10.4, follow these steps to configure the printer function:

1. On the toolbar, click "Go/Utilities".
2. Click "Printer Setup Utility".
3. Click "Add".
4. Hold the "alt" key and click "More Printers".
5. In the pop up window, select "Advanced" and "Windows Printer with SAMBA", enter the printer name and the printer URI (the format is smb://QGW IP/printer name. The printer name is found on the "Device Configuration" > "USB Printer page"), select "Generic" for Printer Model and click "Add".
6. The printer appears on the printer list and is ready to use.

**Note:**

- For "Advanced" in Step 5 above, you must hold the "alt" key and click "More Printers" at the same time to view the Advanced printer settings.
- The network printer service of the QGW series supports Postscript printer on Mac OS only.

## Linux (Ubuntu 10.10)

If you are using Linux (Ubuntu 10.10), follow these steps to configure the printer function:

1. Click the "System" tab, choose "Administration". Then select "Printing".
2. Click "Add".
3. Click "Network Printer", and then select "Internet Printing Protocol (ipp)". Enter the QGW system IP address in "Host". "/printers" is already present. Enter the printer name after "printers/" in the field "Queue".
4. Before you continue, click "Verify" to test the printer connection.
5. The operating system starts to search for the possible drivers.
6. Select the printer driver from the built-in database, or search online.
7. Choose the correct printer model and driver. Depending on the printer, some additional printer options may be available in the next step.
8. You can rename this printer or enter additional information. Click "Apply" to exit and finish.
9. The network printer is now available for printing.

# UPS

By enabling UPS (Uninterruptible Power Supply) support, you can protect your QGW series from abnormal system shutdown caused by power disruption. There are two options provided on the "UPS" page for the QGW series during a power failure: 1) turn off the server after the AC power fails, or 2) enter the auto-protection mode after the AC power fails. For option 1, the QGW series will shut itself down after the specified time. For option 2, the QGW series will stop all running services and unmount all volumes to protect your data after the specified time. For details on QGW system behavior during a power failure, refer to the "Behavior of the UPS Feature of the QGW Series" section. Please note that to protect your data, once the power outage starts, the QGW series will automatically turn itself off or enter auto-protection mode (depending on your settings) after 30 seconds regardless of the specified time for either of the above options if the remaining UPS battery charge is < 15%.

In this chapter, the following topics are covered:

- [USB Modes](#)
  - [Standalone Mode – USB](#)
  - [Standalone Mode – SNMP](#)
  - [Network Master Mode](#)
  - [Network Slave Mode](#)
- [Behavior of the UPS Feature of the QGW Series](#)

## USB Modes

### Standalone Mode – USB

To operate under USB standalone mode, follow the steps below:

1. Plug in the USB cable on the UPS to the QGW series.
2. Choose between whether the QGW series will shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the QGW series should wait before executing the option you have selected. After the QGW series enters auto-protection mode, the QGW series resumes the previous operation status when the power restores.
3. Click "Apply All" to confirm.

### Standalone Mode – SNMP

To operate under SNMP standalone mode, follow the steps below:

1. Make sure the QGW series is connected to the same physical network as the SNMP-based UPS.
2. Select "APC UPS with SNMP management" from the "Protocol" drop down menu.
3. Enter the IP address of the SNMP-based UPS.

4. Choose between whether the QGW series should shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the QGW series should wait before executing the option you have selected. After the QGW series enters auto-protection mode, the QGW series resumes the previous operation status when the power restores.
5. Click "Apply All" to confirm.

### **Network Master Mode**

A network UPS master is responsible for communicating with network UPS slaves on the same physical network regarding critical power status. To set your QGW series with UPS as network master mode, plug in the USB cable on the UPS to the QGW series and follow these steps:

1. Make sure the QGW series (the "UPS master") is connected to the same physical network as the network UPS slaves.
2. Click "Enable network UPS Support". This option only appears when your QGW series is connected to the UPS by a USB cable.
3. Choose between whether the QGW series should shut down or enter auto-protection mode after the AC power fails. Specify the time in minutes that the QGW series should wait before executing the option you have selected. After the QGW series enters auto-protection mode, the QGW series resumes the previous operation status when the power restores.
4. Enter the "IP address" of other network UPS slaves to be notified in the event of power failure.
5. Click "Apply All" to confirm and continue the setup for the QGW systems which operate in network slave mode below.

### **Network Slave Mode**

A network UPS slave communicates with network UPS master to receive the UPS status. To set up your QGW series with UPS as network slave mode, follow these steps:

1. Make sure the QGW series is connected to the same physical network as the network UPS master.
2. Select "Network UPS slave" from the "Protocol" drop down menu.
3. Enter the IP address of the network UPS server.
4. Choose between whether the QGW series should shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the QGW series should wait before executing the option you have selected. After the QGW series enters auto-protection mode, the QGW series resumes the previous operation status when the power restores.
5. Click "Apply All" to confirm.

**Note:** To allow the UPS device to send SNMP alerts to the QGW series in the event of power loss, you may have to enter the QGW system IP address in the UPS configuration page.

## Behavior of the UPS Feature of the QGW Series

There are three phases during a power outage:

- Phase 1: Power loss starts until the end of the waiting time.
- Phase 2: From the end of the waiting time to the point when the UPS device runs out of its battery.
- Phase 3: After the UPS device runs out of its battery and until the power restores.

### Phase 1:

As soon as the power loss starts, the QGW series will detect the UPS device's battery. If the remaining UPS battery charge is < 15%, the system will automatically turn itself off or enter auto-protection mode (depending on your settings) after 30 seconds regardless the time you specified for either of the settings (turn off the QGW series or enter auto protection mode.) If the UPS battery charge is > 15%, the QGW series will wait for the specified time you entered in the "UPS" page.

If the power resumes during this phase, the QGW series will remain in operation.

### Phase 2:

Depending on your setting on the "UPS" page:

- If in auto-protection mode, the QGW series will stop all running services and unmount all volumes. The QGW series at this moment will become inaccessible.
- If the QGW series is powered off, it will remain off.

If the power resumes during this phase:

- If in auto-protection mode, the QGW series will reboot and resume its previous state.
- If the QGW series is powered off, it will remain off.

### Phase 3:

Depending on your setting on the "UPS" page:

- If in auto-protection mode, the QGW series will lose its power and shut down.
- If the QGW series is powered off, it will remain off.

After the power resumes during this phase, the QGW series will react according to your settings in "System Settings" > "Power Recovery".

# System Status

Go to "Control Panel" > "System Settings" > "System Status" to check the status of your QGW series.

System Information	Network Status	System Service	Hardware Information	Resource Monitor
<b>Summary</b>				
Server name	NASC4EF14			
Model name	TS-259 Pro+			
Serial number	Q108100567			
Total memory	997.2 MB			
Firmware version	4.2.1 Build 20151214			
System up time	0 day 8 Hour 30 Minute(s)			
Time zone	(GMT+08:00) Taipei			
Filename encoding	English			

## System Information

View the summary of system information such as the server name, CPU, memory, firmware and system up time on this page.

## Network Status

View the current network settings and statistics on this page. They are displayed based on network interface. Click the up arrow in the top right to collapse the interface page and the down arrow to expand it.

## System Service

View the current settings of system services provided by the QGW series.

## Hardware Information

View basic hardware information of the QGW series.

## Resource Monitor

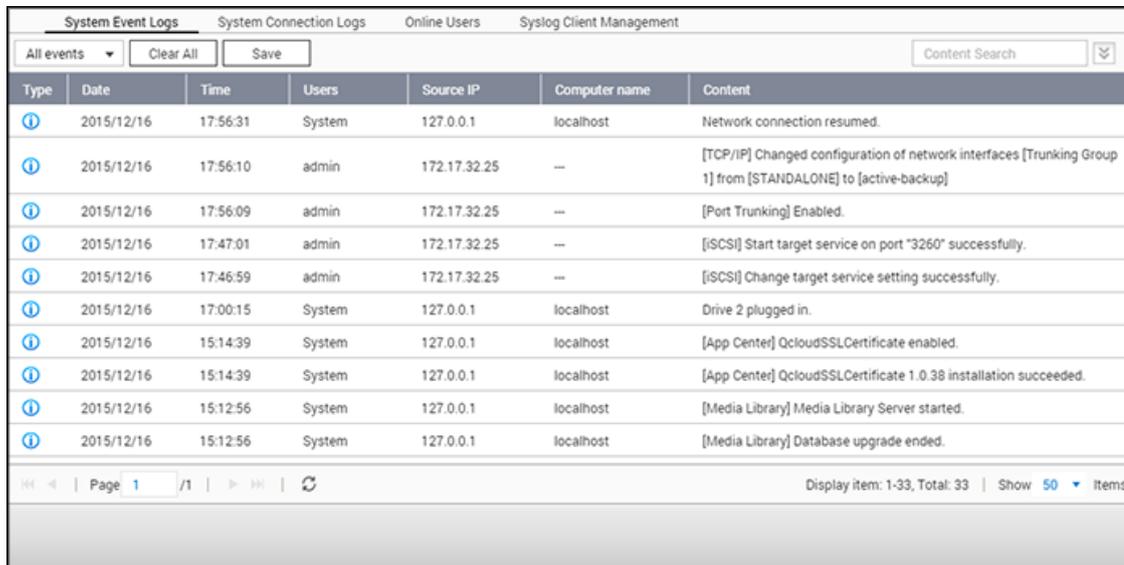
You can view the CPU usage, disk usage, and bandwidth transfer statistics of the QGW series.

- CPU Usage: Shows the CPU usage of the QGW series.

- Memory Usage: Shows the memory usage of the QGW series by real-time dynamic graph.
- Disk Usage: Shows the disk space usage of each disk volume and its shared folders.
- Bandwidth Usage: Provides bandwidth transfer information of each available QGW system LAN port.
- Process: Shows information about the processes running on the QGW series.
- Disk Performance: Shows IOPS and latency of the selected volume.

# System Logs

Go to "Control Panel" > "System Settings" > "System Logs" to configure the logs settings of your QGW series.



The screenshot shows the "System Event Logs" interface. At the top, there are tabs for "System Event Logs", "System Connection Logs", "Online Users", and "Syslog Client Management". Below the tabs, there are buttons for "All events", "Clear All", and "Save", along with a "Content Search" field. The main area is a table with the following columns: Type, Date, Time, Users, Source IP, Computer name, and Content. The table contains 11 rows of log entries. At the bottom, there is a pagination bar showing "Page 1 / 1" and "Display item: 1-33, Total: 33 | Show 50 Items".

Type	Date	Time	Users	Source IP	Computer name	Content
ⓘ	2015/12/16	17:56:31	System	127.0.0.1	localhost	Network connection resumed.
ⓘ	2015/12/16	17:56:10	admin	172.17.32.25	--	[TCP/IP] Changed configuration of network interfaces [Trunking Group 1] from [STANDALONE] to [active-backup]
ⓘ	2015/12/16	17:56:09	admin	172.17.32.25	--	[Port Trunking] Enabled.
ⓘ	2015/12/16	17:47:01	admin	172.17.32.25	--	[iSCSI] Start target service on port "3260" successfully.
ⓘ	2015/12/16	17:46:59	admin	172.17.32.25	--	[iSCSI] Change target service setting successfully.
ⓘ	2015/12/16	17:00:15	System	127.0.0.1	localhost	Drive 2 plugged in.
ⓘ	2015/12/16	15:14:39	System	127.0.0.1	localhost	[App Center] QcloudSSLCertificate enabled.
ⓘ	2015/12/16	15:14:39	System	127.0.0.1	localhost	[App Center] QcloudSSLCertificate 1.0.38 installation succeeded.
ⓘ	2015/12/16	15:12:56	System	127.0.0.1	localhost	[Media Library] Media Library Server started.
ⓘ	2015/12/16	15:12:56	System	127.0.0.1	localhost	[Media Library] Database upgrade ended.

## System Event Logs

The QGW series can store 10,000 recent event logs, including warnings, errors, and information. If the QGW series does not function correctly, refer to the event logs for troubleshooting.

**Tip:** Right click on a record to delete it. To clear every log, click "Clear All".

## System Connection Logs

The QGW series can record HTTP, FTP, Telnet, SSH, AFP, and SAMBA connections. Click "Options" to select the connection type to be logged. File transfer performance may be slightly impacted when this feature is enabled.

**Tip:** Right click on a record and select to delete the record or to block the IP and select how long the IP should be blocked. To clear every log, click "Clear All".

**Start Logging:** Enable this option to archive connection logs. When the number of logs reaches the upper limit the QGW series will automatically generate a CSV file and save it to a specified folder. File-level access logs are available on this page. The QGW series will record logs when users access, create, delete, move, or rename any files/folders via the connection type specified in "Options". To disable this feature, click "Stop logging".

**Note:** For AFP and SSH connections, the system can only record login and logout events.

## Online Users

The information of online users connected to the QGW series by networking services is shown here.

**Tip:** Right click on a record to disconnect the IP connection and block the IP.

## Syslog Client Management

Syslog is a standard for forwarding log messages on an IP network. Enable this option to save event and connection logs to a remote Syslog server. When converting connection logs into a CSV file, the connection type and action will be number coded. Refer to the table for code meanings.

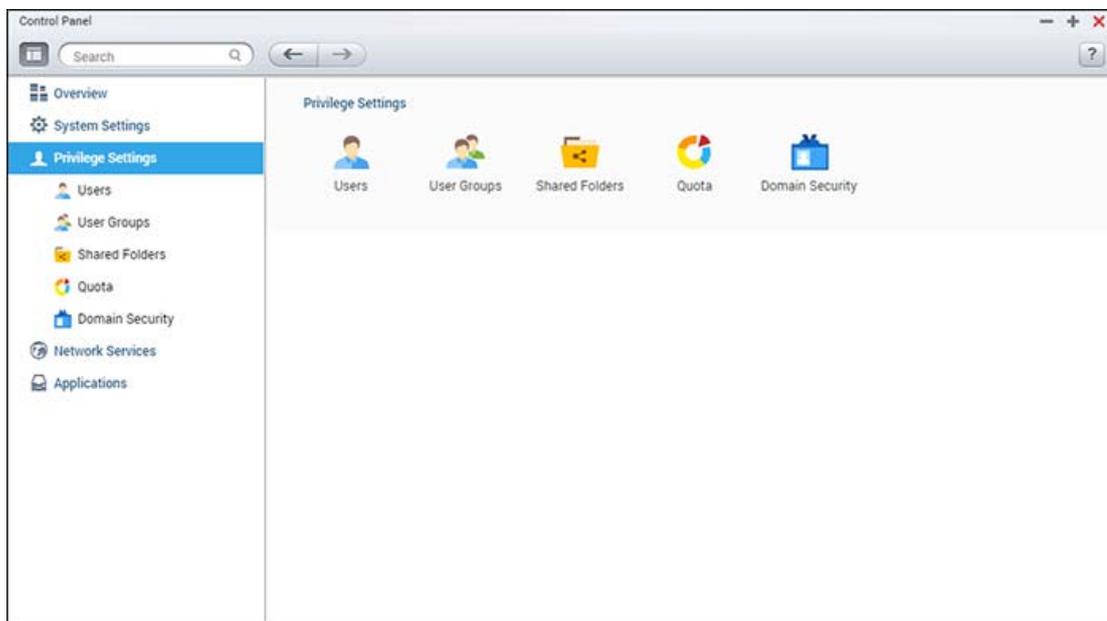
Connection type codes	Action codes
0 - UNKNOWN	0 - UNKNOWN
1 - SAMBA	1 - DEL
2 - FTP	2 - READ
3 - HTTP	3 - WRITE
4 - NFS	4 - OPEN
5 - AFP	5 - MKDIR
6 - TELNET	6 - NFSMOUNT_SUCC
7 - SSH	7 - NFSMOUNT_FAIL
	8 - RENAME
	9 - LOGIN_FAIL
	10 - LOGIN_SUCC
	11 - LOGOUT
	12 - NFSUMOUNT
	13 - COPY
	14 - MOVE
	15 - ADD

## Advanced Log Search

Advanced log search is provided to search for system event logs, system connection logs and online users based on user preferences. First, specify the log type, users, computer name, date range and source IP and click "Search" to search for desired logs or reset to list all logs. Please note that for online users, only the source IP and Computer name can be specified.

# Privilege Settings

Go to "Control Panel" > "Privilege Systems" to configure privilege settings, disk quotas and domain security on the QGW series.



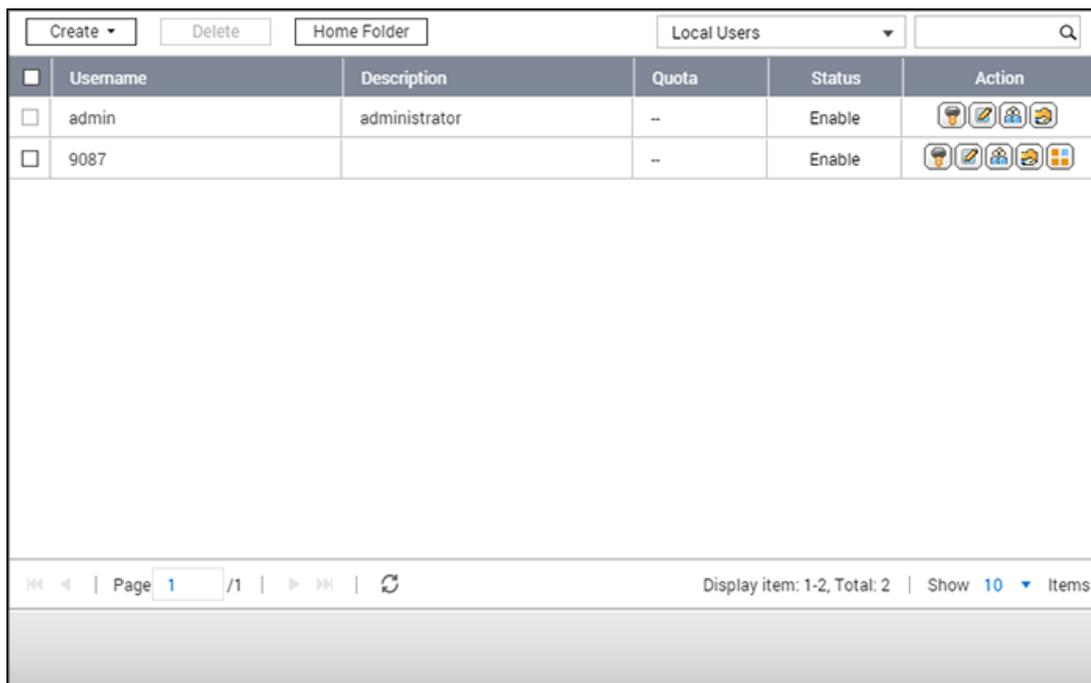
For setup details, refer to the following links:

- [Users](#)
- [User Groups](#)
- [Share Folders](#)
- [Quota](#)
- [Domain Security](#)
- [Domain Controller](#)

# Users

The QGW series creates the following users by default:

- admin: The administrator "admin" has full access to system administration and all shared folders. It cannot be deleted.
- guest: This is a built-in user and will not be displayed on the "User Management" page. A guest does not belong to any user group. The login password is "guest".
- anonymous: This is a built-in user and will not be shown on the "User Management" page. When you connect to a QGW system by FTP, you can use this name to login.



The screenshot shows a web interface for managing local users. At the top, there are buttons for 'Create', 'Delete', and 'Home Folder', along with a dropdown menu for 'Local Users' and a search icon. Below this is a table with the following columns: Username, Description, Quota, Status, and Action. Two users are listed: 'admin' with description 'administrator' and '9087'. Both have a status of 'Enable' and a quota of '--'. The Action column contains icons for edit, delete, and other functions. At the bottom, there is a pagination bar showing 'Page 1 / 1' and 'Display item: 1-2, Total: 2 | Show 10 Items'.

<input type="checkbox"/>	Username	Description	Quota	Status	Action
<input type="checkbox"/>	admin	administrator	--	Enable	
<input type="checkbox"/>	9087		--	Enable	

The following information is required to create new users:

- Username: The username is case-insensitive and supports multi-byte characters, such as Chinese, Japanese, Korean, and Russian. The maximum length is 32 characters. Invalid characters are: " / \ [ ] : ; | = , + \* ? < > ` ' "
- Password: The password is case-sensitive. It is recommended to use a password of at least 6 characters. The maximum length is 64 characters.

In this chapter, the following topics are covered:

- [Creating a User](#)
- [Creating Multiple Users](#)
- [Importing/Exporting Users](#)
- [Home Folders](#)

## Creating a User

To create a user on the QGW series, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Create a User".
3. Follow the wizard instructions to complete the details.

## Creating Multiple Users

To create multiple users on the QGW series, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Create Multiple Users".
3. Click "Next".
4. Enter the name prefix (for example: "test".) Enter the start number for the username, e.g. 0001 and the number of users to be created (for example: 10.) The QGW series will then create ten users named: test0001, test0002, test0003 ... test0010. The password entered here is the same for all the new users.
5. Select to create a private shared folder for each user or not. The shared folder will be named after the username. If a shared folder of the same name has already existed, the QGW series will not create the folder.
6. Specify the folder settings.
7. You can view the new users created in the last step. Click "Finish" to exit the wizard.
8. Check that the users have been created.
9. Check that the shared folders have been created for the users.

## Importing/Exporting Users

You can import users to or export users from the QGW series with this function.

### Exporting users

Follow the steps below to export users from the QGW series:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Import/Export Users".
3. Select the option "Export user and user group settings".
4. Click "Next" to download and save the account setting file (\*.bin.) This file can be imported to another QGW system for account setup.

### Importing users

Before importing users to the QGW series, make sure you have backed up the original users' settings by exporting the users. Follow these steps to import users to the QGW series:

1. Go to "Control Panel" > "Privilege Settings" > "Users".
2. Click "Create" > "Import/Export Users".
3. Select "Import user and user group settings". Select the option "Overwrite duplicate users" to overwrite existing users on the QGW series. Click "Browse", select the file (\*.txt, \*.csv, \*.bin) which contains the users' information and click "Next" to import the users.
4. Click "Finish" after the users have been created.
5. The imported user accounts will be displayed.

**Note:**

- The password rules (if applicable) will not be applied when importing users.
- The quota settings can be only exported when the quota function is enabled in "Privilege Settings" > "Quota".

The QGW series supports importing user accounts from TXT, CSV or BIN files. To create a list of user accounts with these file types, follow these steps:

**TXT**

1. Open a new file with a text editor.
2. Enter a user's information in the following order and separate them by ",": Username, Password, Quota (MB), Group Name
3. Go to the next line and repeat the previous step to create another user account. Each line indicates one user's information.
4. Save the file with UTF-8 encoding if it contains double-byte characters.

Note that if the quota is left empty, the user will have no limit in using the disk space of the QGW series.

**CSV (Excel)**

1. Open a new file with Excel.
2. Enter a user's information in the same row in the following order:
  - Column A: Username
  - Column B: Password
  - Column C: Quota (MB)
  - Column D: Group name
3. Go to the next row and repeat the previous step to create another user account. Each row indicates one user's information. Save it as a CSV file.
4. Open the CSV file with Notepad and save it in UTF-8 encoding if it contains double-byte characters.

### **BIN (Exported from the QGW series)**

The BIN file is exported from a QGW system. It contains information including username, password, quota, and user group. The quota setting can only be exported when the quota function is enabled in "Privilege Settings" > "Quota".

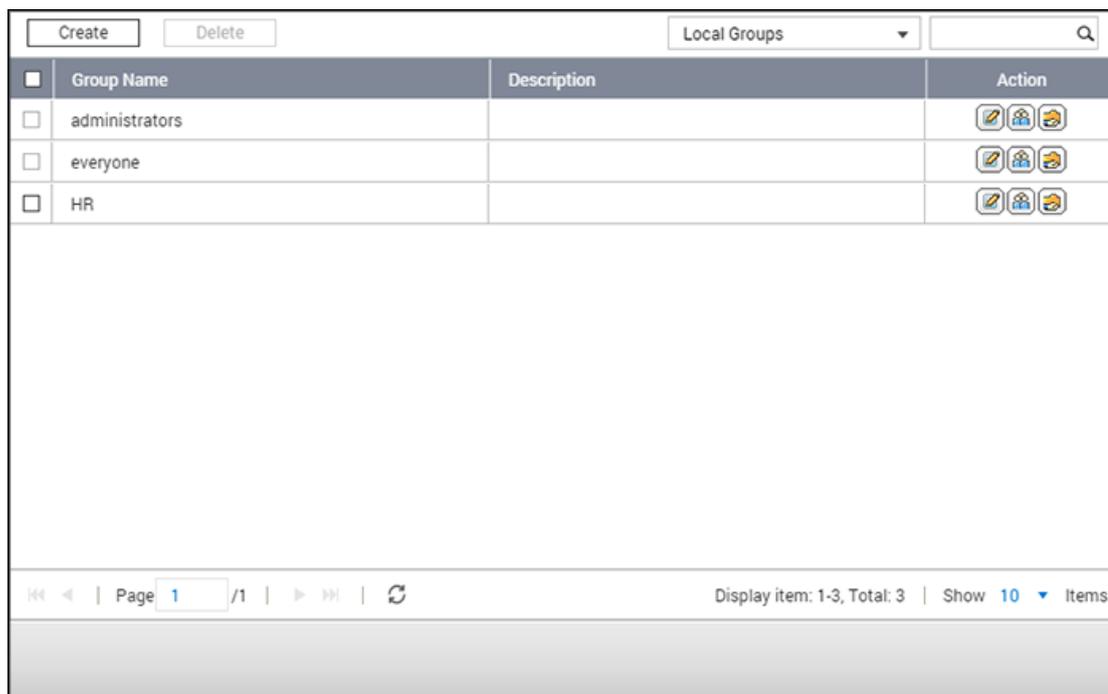
### **Home Folders**

Enable Home Folders to create a personal folder to each local and domain user on the QGW series. Users can access their home folders via Microsoft networking, FTP, AFP, and File Station. All the home folders are located in the shared folder "Homes", which can only be accessed by "admin" by default.

To use this feature, click "Home Folders". Select "Enable home folder for all users" and the disk volume where the home folders will be created in. Click "Apply".

# User Groups

A user group is a collection of users with the same access rights to files or folders.



<input type="checkbox"/>	Group Name	Description	Action
<input type="checkbox"/>	administrators		  
<input type="checkbox"/>	everyone		  
<input type="checkbox"/>	HR		  

The QGW series creates the following user groups by default:

- administrators: All the members in this group have administration rights of the QGW series. This group cannot be deleted.
- everyone: All the registered users belong to this group. This group cannot be deleted.

A group name cannot exceed 256 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones: " / \ [ ] : ; | = , + \* ? < > ` ' .

# Shared Folders

Go to "Control Panel" > "Privilege Settings" > "Shared Folders" to configure shared folders of your QGW series.

<input type="checkbox"/>	Folder Name	Size	Fold...	Files	Hi...	Volume	Action
<input type="checkbox"/>	Download	3.82 MB	3	29	No	DataVol1	
<input type="checkbox"/>	Multimedia	48.89 GB	143	1593	No	DataVol1	
<input type="checkbox"/>	Public	577.55...	28	19	No	DataVol1	
<input type="checkbox"/>	Recordings	417.34...	4	3	No	DataVol1	
<input type="checkbox"/>	Web	32 KB	2	3	No	DataVol1	
<input type="checkbox"/>	homes	236 KB	14	12	No	DataVol1	

This chapter covers the following topics:

- [Shared Folders](#)
- [Folder Encryption](#)
- [ISO Shared Folders](#)
- [Folder Aggregation](#)

## Shared Folders

You can create 256 shared folders on the QGW series and specify the access rights of the users and user groups to the shares.

To create a shared folder, follow the steps below:

1. Click "Create" > "Shared Folder".
2. Enter the basic folder settings.
  - Folder name: Enter the share name. The share name does not support " / \ [ ] : ; | = , + \* ? < > ` '`
  - Comment: Enter an optional description of the shared folder.
  - Disk Volume: Select which disk volume on which to create the folder.
  - Path: Specify the path of the shared folder or select to let the QGW system specify the path automatically.

3. Access privileges for users: Select the way you want to specify access rights to the folder. If you select to specify the access rights by user or user group, you can select to grant read only, read/write, or deny access to the users or user groups.
4. Folder Encryption: Select to enable folder encryption with 256-bit AES encryption. See [Folder Encryption](#) for more information.
5. Advanced settings (this is only available when creating a shared folder)
  - o Guest Access Right: Assign guest access rights of the folder.
  - o Media Folder: Select to set the shared folder as a media folder.
  - o Hidden Folder Hide Network drive: Select to hide the shared folder or not in Microsoft Networking. When a shared folder is hidden, you have to enter the complete directory \\QGW\_IP\share\_name to access the share.
  - o Lock File (Oplocks): Opportunistic locking is a Windows mechanism for the client to place an opportunistic lock (oplock) on a file residing on a server in order to cache the data locally for improved performance. Oplocks is enabled by default for everyday usage and should be disabled on networks that require multiple users concurrently accessing the same files.
  - o SMB Encryption: Set the folder to be accessible for SMB 3 clients. This option is only available after SMB3 is enabled. After it is enabled, all communications via Microsoft Networking will be conducted via SMB3 and encrypted. All SMB3 clients will be able to connect to QGW series via Microsoft Networking.
  - o Recycle Bin: Enable the Network Recycle Bin for created shared folders. "Restrict the access of Recycle Bin to administrators only for now" will ensure that files deleted and moved to the Network Recycle Bin can only be recovered by administrators. Please note that the Recycle Bin option is only available after you enable Network Recycle Bin in "Control Panel" > "Network Services" > "Network Recycle Bin".
  - o Enable Sync on this shared folder: Enable this option if you want to sync the contents in this shared folder. Refer to [Qsync Central Station](#) for more details.
6. Click "create" to complete the setup.

To delete a shared folder, select the folder checkbox and click "Remove". You can select the option "Also delete the data. (Mounted ISO image files will not be deleted)" to delete the folder and the files in it. If you do not select to delete the folder data, the data will be retained in the QGW series. You can create a shared folder of the same name again to access the data.

Icon	Name	Description
	Folder Property	Edit the folder property. Select to hide or show the network drive, enable or disable oplocks, folder path, comment, restrict the access of Recycle Bin to administrators (files can only be recovered by administrators from the Network Recycle

		Bin) ,enable or disable write-only access on FTP connection, folder encryption, and synchronization.
	Folder Permissions	Edit folder permissions and subfolder permissions.
	Refresh	Refresh the shared folder details.

**Folder Permissions**

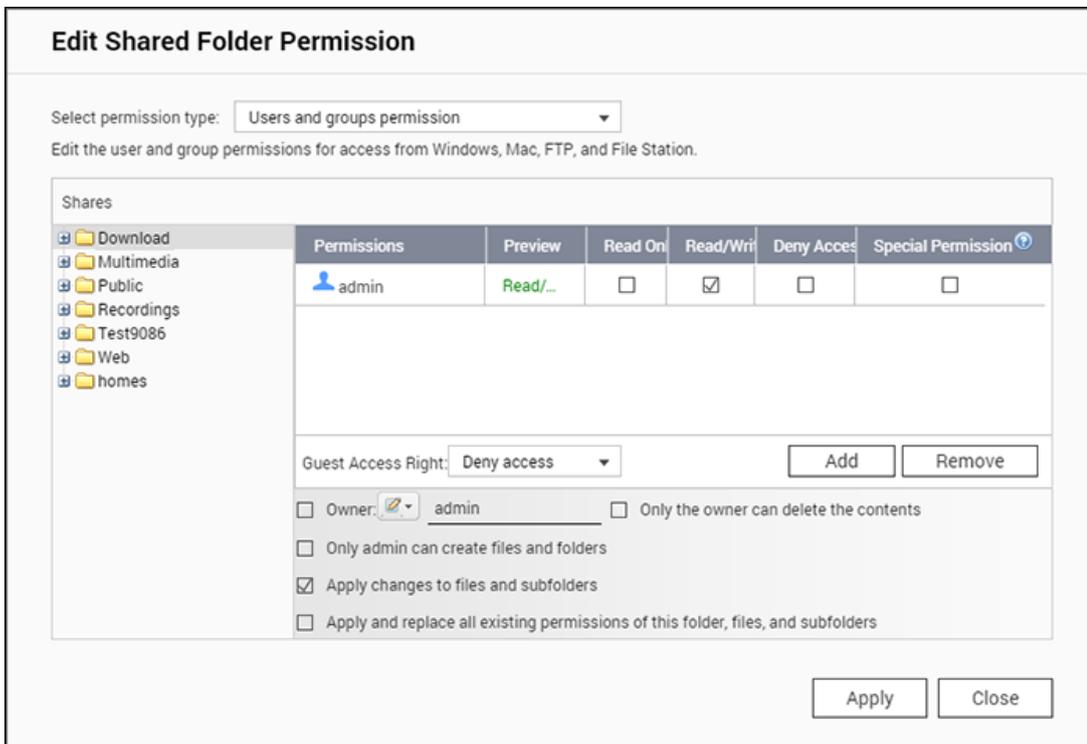
Configure folder and subfolder permissions on the QGW series. To edit basic folder permissions, locate a folder name in "Privilege Settings" > "Shared Folders" and click "Folder Permissions". The folder name will be shown on the left and the users with configured access rights are shown in the panel. You can also specify guest access rights on the bottom of the panel. Click "Add" to select more users and user groups and specify their access rights to the folder. Click "Add" to confirm. Click "Remove" to remove any configured permissions. You can select multiple items by holding the Ctrl key and left clicking the mouse. Click "Apply" to save the settings.

**Subfolder Permissions**

The QGW series supports subfolder permissions for secure management of the folders and subfolders. You can specify read, read/write, and deny access of individual user to each folder and subfolder.

To configure subfolder permissions, follow the steps below:

1. Go to "Privilege Settings" > "Shared Folders" > "Advanced Permissions" tab. Select "Enable Advanced Folder Permissions" and click "Apply".
2. Go to "Privilege Settings" > "Shared Folders" > "Shared Folders" tab. Select a root folder, for example Dept, and click "Folder Permissions". The shared folder name and its first-level subfolders are shown on the left. The users with configured access rights are shown in the panel, with special permission below. Double click the first-level subfolders to view the second-level subfolders. Select the root folder (Dept). Click "+ Add" to specify read only, read/write, or deny access for the users and user groups.
3. Click "Add" when you have finished the settings.
4. Specify other permissions settings below the folder permissions panel.
  - o Guest Access Right: Specify to grant full or read only access or deny guest access.
  - o Owner: Specify the owner of the folder. By default, the folder owner is the creator.
5. To change the folder owner, click the "Folder Property" button next to the owner field.



6. Select a user from the list or search a username. Then click "Set".
  - o Only the owner can delete the contents: When you apply this option to a folder, e.g. Dept, only the folder owner can delete the first-level subfolders and files. Users who are not the owner but possess read/write permission to the folder cannot delete the folders Admin, HR, Production, Sales, and test in this example. This option does not apply to the subfolders of the selected folder even if the options "Apply changes to files and subfolders" and "Apply and replace all existing permissions of this folder, files, and subfolders" are selected.
  - o Only admin can create files and folders: This option is only available for root folders. Select this option to allow admin to create first-level subfolders and files in the selected folder only. For example, in the folder "Dept", only admin can create files and subfolders Admin, HR, Production, and so on. Other users with read/write access to Dept can only create files and folders in the second and lower-level subfolders such as Admin01, Admin02, HR1, and HR2.
  - o Apply changes to files and subfolders: Apply permissions settings except owner protection and root folder write protection settings to all the files and subfolders within the selected folder. These settings include new users, deleted users, modified permissions, and folder owner. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.
  - o Apply and replace all existing permissions of this folder, files, and subfolders: Select this option to override all previously configured permissions of the selected folder and its files and subfolders except owner protection and root folder write protection settings. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.

- Special Permission: This option is only available for root folders. Select this option and choose between "Read only" or "Read/Write" to allow a user to access to all the contents of a folder irrespectively of the pre-configured permissions. A user with special permission will be identified as "admin" when he/she connects to the folder via Microsoft Networking. If you have granted special permission with "Read/Write" access to the user, the user will have full access and is able to configure the folder permissions on Windows. Note that all the files created by this user belong to "admin". Since "admin" does not have quota limit on the QGW series, the number and size of the files created by users with special permission will not be limited by their pre-configured quota settings. This option should be used for administrative and backup tasks only.

7. After changing the permissions, click "Apply" and then "YES" to confirm.

**Note:**

- You can create up to 230 permission entries for each folder when Advanced Folder Permission is enabled.
- If you have specified "deny access" for a user on the root folder, the user will not be allowed to access the folder and subfolders even if you select read/write access to the subfolders.
- If you have specified "read only access" for a user on the root folder, the user will have read only access to all the subfolders even if you select read/write access to the subfolders.
- To specify read only permission on the root folder and read/write permission on the subfolders, you must set read/write permission on the root folder and use the option "Only admin can create files and folders" (to be explained later).
- If an unidentified account ID (such as 500) is shown for a subfolder on the permission assignment page after you click the "Access Permissions" button next to a shared folder in "Control Panel">"Privilege Settings">"Shared Folders">"Shared Folder", it is likely that the permission of that subfolder has been granted to a user account that no longer exists. In this case, please select this unidentified account ID and click "Remove" to delete it.

**Microsoft Networking Host Access Control**

QGW folders can be accessed via Samba (Windows) by default. You can specify authorized IP addresses and hosts by following these steps:

1. Click "Folder Permissions".
2. Select "Microsoft Networking host access" from the drop-down menu on top of the page.
3. Specify the allowed IP addresses and host names. The following IP address and host name are used as example here:
  - IP address: 192.168.12.12 or 192.168.\*.\*

- Host name: dnsname.domain.local or \*.domain.local

4. click "Add" to enter the IP address and host name and then "Apply".

#### **Notifications on characters used:**

- Wildcard characters: You can enter wildcard characters in an IP address or host name entry to represent unknown characters.
- Asterisk (\*): Use an asterisk (\*) as a substitute for zero or more characters. For example, if you enter \*.domain.local, the following items are included: a.domain.local, cde.domain.local, or test.domain.local
- Question mark (?): Use a question mark (?) as a substitute for only one character. For example, test?.domain.local includes the following: test1.domain.local, test2.domain.local, or testa.domain.local

When you use wildcard characters in a valid host name, dot (.) is included in wildcard characters. For example, when you enter \*.example.com, "one.example.com" and "one.two.example.com" are included.

#### **Folder Encryption**

Shared folders on the QGW series can be encrypted with 256-bit AES encryption to protect data. The encrypted shared folders can only be mounted for normal read/write access with the authorized password. The encryption feature protects the confidential data of the folder from unauthorized access even if the hard drives or the entire QGW system were stolen.

##### **Note:**

- The function or its content is only applicable on some models.
- The encryption key cannot include dollar signs (\$) or equal signs (=).
- Encrypted shared folders cannot be accessed via NFS.
- If a volume has been encrypted, the shared folders on that volume can not be encrypted.

#### **Encrypting and locking a shared folder**

To encrypt and lock a shared folder, follow these steps:

1. Enable folder encryption:
  - When you create a folder, tick "Encryption" under "Folder Encryption", enter a password and choose to save an encryption key.
  - To encrypt an existing folder, click "Edit Properties" under "Action" in "Control Panel" > "Privilege Settings" > "Shared Folders", tick "Encrypt this folder", enter a password and choose to save encryption key.

2. Go to "Control Panel" > "Privilege Settings" > "Shared Folders", click "Encryption Management" under "Action".
3. Switch to "Lock" and click "OK".

### Encryption verification

After a folder is locked, that folder will be invisible in File Station. If an encrypted shared folder is unlocked, it will reappear in File Station.

### Unlocking a shared folder

To unlock an encrypted and locked shared folder, go to "Control Panel" > "Privilege Settings" > "Shared Folders", click "Encryption Management" under "Action" and enter the password or upload the encryption key file.

### Encryption Management

After the folder is encrypted, click "Encryption Management" under "Action" in "Control Panel" > "Privilege Settings" > "Shared Folders" to edit encryption settings:

- To save the encryption key, select the "Download" tab and enter the encryption password to export the key.
- You can choose to automatically mount the encrypted folder by selecting "Mount automatically on start up" in the "Save" tab. Enter the encryption key to mount the folder automatically for access. This option will be automatically enabled if the "Save encryption key" is checked when encrypting the folder. Folders that do not have this option enabled will be locked after the system restarts.
- To prevent access to the encrypted folder, enable the lock function in the "Lock" tab. Select "Forget the saved key" if you want the folder to remain locked after the system restarts (i.e., without auto mount when system starts.) To unlock the folder later, click "Unlock Share Folder" and then enter or import the encryption key to unlock the folder.

#### Note:

- It is strongly recommended that you export and save the encryption key. You need the key to unlock or decrypt the encrypted folder.
- You cannot change an encrypted folder's volume or path.
- QGW series also offers volume-based encryption. See [Volume Encryption](#) for more details.
- The default shared folders cannot be encrypted.

### ISO Shared Folders

You can mount ISO image files on the QGW series as ISO shares. The QGW series supports mounting up to 256 ISO shares.

Follow these steps to mount an ISO file on the QGW series using the web interface:

1. Log into the QGW series as an administrator. Go to "Share Folders" > "Create". Click "Create an ISO Share".
2. Select an ISO image file on the QGW series. Click "Next".
3. The image file will be mounted as a shared folder of the QGW series. Enter the folder name.
4. Specify the access rights of QGW users or user groups to the shared folder. You can also select "Deny Access" or "Read only" for the guest access right. Click "Next".
5. Confirm the settings and click "Next".
6. Click "Finish".
7. After mounting the image file, you can specify access rights for users over different network protocols such as SMB, AFP, NFS, and WebDAV by clicking the Access Permission icon in the "Action" column.

The QGW series supports mounting ISO image files using File Station. Refer to the [File Station](#) chapter for more details.

**Note:**

For Mac OSX, mounting a folder that contains the # character in the folder name through WebDAV is not supported. Please rename the folder before mounting it if necessary.

## Folder Aggregation

You can aggregate the shared folders on Microsoft network as a portal folder on the QGW series and let users access the folders through your QGW series. Up to 10 folders can be linked to a portal folder. To use this function, follow these steps:

1. Enable folder aggregation.
2. Click "Create a Portal Folder".
3. Enter the portal folder name. Select to hide the folder or not, and enter an optional comment for the portal folder. Select the option "User must login before accessing the portal folder" to avoid guest access and permission issues on the shared folders.
4. Click the "Link Configuration" button under "Action" and enter the remote folder settings. Make sure the folders are open for public access.
5. Upon successful connection, you can connect to the remote folders through the QGW series.

**Note:**

- Folder Aggregation is only supported in Microsoft networking service and is recommended for a Windows AD environment.
- If there is permission control on the folders, you need to join the QGW system and the remote servers to the same AD domain.

**Advanced Permissions**

"Advanced Folder Permissions" and "Windows ACL" provide subfolder and file level permissions control. They can be enabled independently or together.

Protocols	Permission	Options	How to Configure
Advanced Folder Permissions	FTP, AFP, File Station, Samba	3 (Read, Read & Write, Deny)	QGW web UI
Windows ACL	Samba	13 (NTFS permissions)	Windows File Explorer
Both	FTP, AFP, File Station, Samba	Please see the application note ( <a href="https://www.qnap.com/i/en/trade_tech/con_show.php?op=showone&amp;cid=6">https://www.qnap.com/i/en/trade_tech/con_show.php?op=showone&amp;cid=6</a> ) for more details.	Windows File Explorer

**Advanced Folder Permissions**

Use "Advanced Folder Permissions" to directly configure subfolder permissions on the QGW series. There is no depth limitation for subfolder permission, but it is highly recommended to only change permissions on the first or second subfolder level. When "Advanced Folder Permissions" is enabled, click "Folder Permissions" under the "Shared Folders" tab to configure subfolder permission settings. See "Shared Folders" > "Folder Permission" of this section for details.

**Windows ACL**

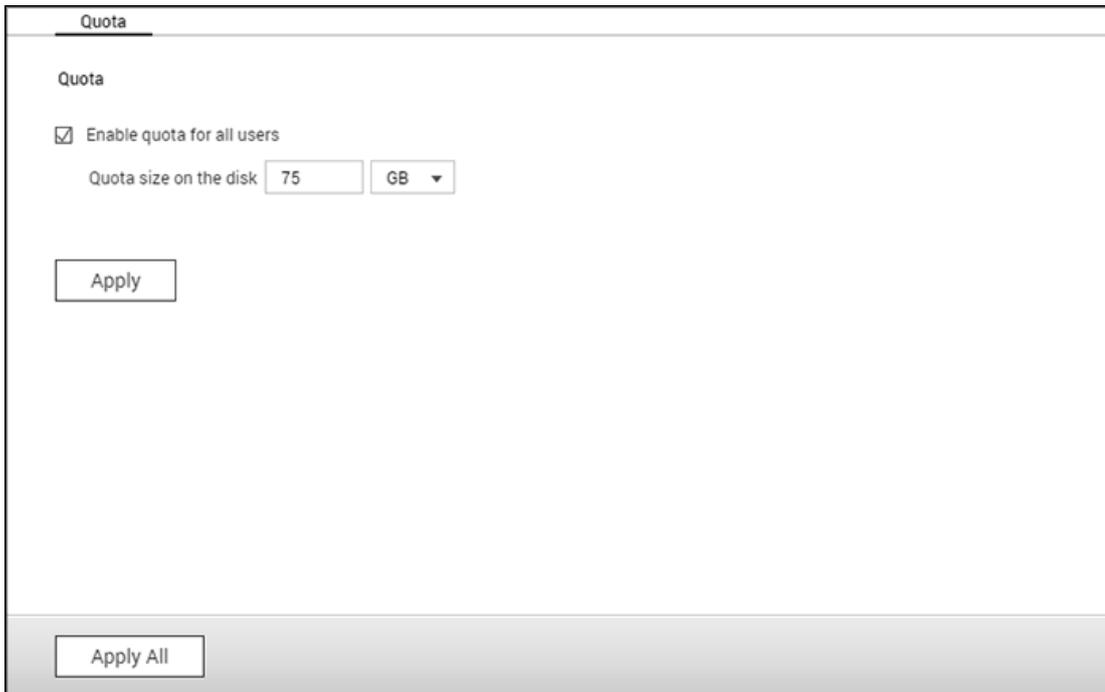
Use "Windows ACL" to configure the subfolder and file level permissions from Windows File Explorer. All Windows Permissions are supported. For detailed Windows ACL behavior, please refer to standard NTFS permissions: <http://www.ntfs.com/ntfs-permissions.htm>

- To assign subfolder and file permissions to a user or a user group, full control share-level permissions must be granted to the user or user group.

- When Windows ACL is enabled when "Advanced Folder Permissions" is disabled, subfolder and file permissions will only have effect when accessing the QGW series from Windows File Explorer. Users connecting to the QGW series via FTP, AFP, or File Station will only have share-level permissions.
- When Windows ACL and Advanced Folder Permissions are both enabled, users cannot configure Advanced Folder Permissions from the QGW series. Permissions (Read only, Read/Write, and Deny) of Advanced Folder Permissions for AFP, File Station, and FTP will automatically follow Windows ACL configuration.

# Quota

To efficiently allocate storage space, you can specify quotas that can be used by each user.



The screenshot shows a web interface for configuring quotas. At the top, there is a tab labeled "Quota". Below the tab, the word "Quota" is displayed. There is a checked checkbox labeled "Enable quota for all users". Below this, there is a label "Quota size on the disk" followed by a text input field containing the number "75" and a dropdown menu currently set to "GB". At the bottom left of the main content area, there is an "Apply" button. At the bottom of the entire interface, there is a grey bar containing an "Apply All" button.

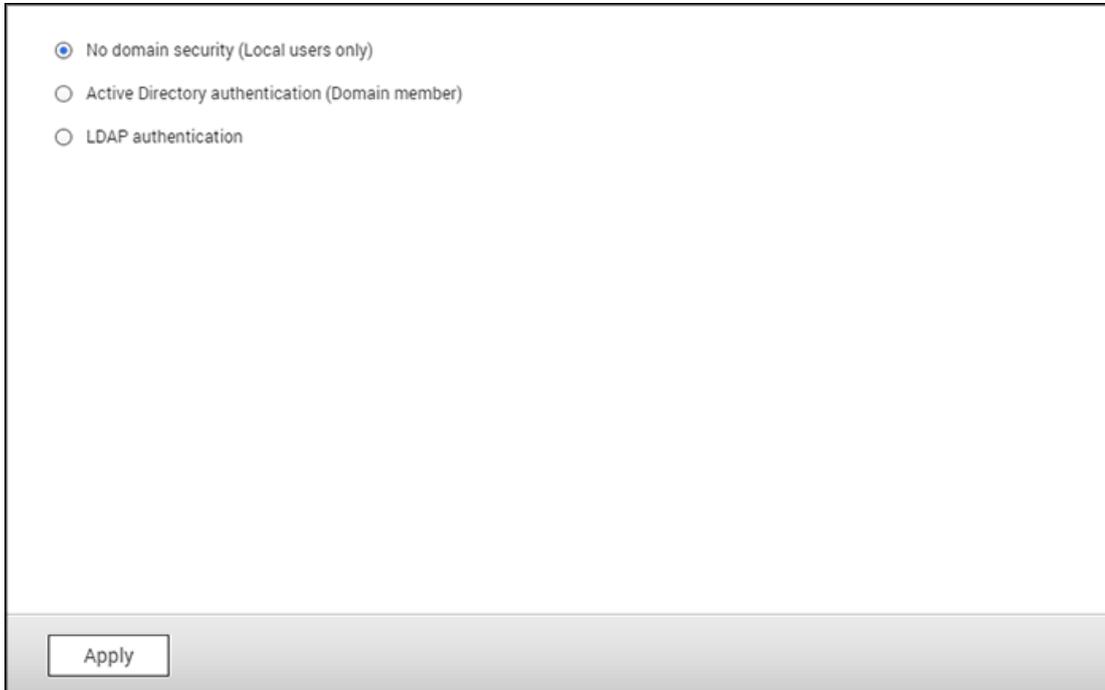
When this is enabled and a user has reached the quota, the user cannot upload any more data to the QGW series. By default, no limitations are set for the users. You can modify the following options:

- Enable quota for all users
- Quota size on each disk volume

After applying the changes, the quota settings will be shown. Click "Generate" to generate a quota settings file in CSV format. After the file has been generated, click "Download" to save it to your specified location.

# Domain Security

The QGW series supports user authentication by local access right management, Microsoft Active Directory (Windows Server 2003/2008/2012), and Lightweight Directory Access Protocol (LDAP) directory.



The screenshot shows a configuration window for Domain Security. It contains three radio button options:

- No domain security (Local users only)
- Active Directory authentication (Domain member)
- LDAP authentication

An "Apply" button is located at the bottom left of the window.

By joining the QGW series to an Active Directory or a LDAP directory, the AD or LDAP users can access the QGW series using their own accounts without extra user account setup on the QGW series.

- **No domain security:** Only the local users can access the QGW series.
- **Active Directory authentication (domain members):** Join the QGW series to an Active Directory. The domain users can be authenticated by the QGW series. After joining the QGW series to an AD domain, both the local QGW users and AD users can access the QGW series via the following protocols/services:
  - Samba (Microsoft Networking)
  - AFP
  - FTP
  - File Station
- **LDAP authentication:** Connect the QGW series to an LDAP directory. The LDAP users can be authenticated by the QGW series. After connecting the QGW series to an LDAP directory, either the local QGW users or the LDAP users can be authenticated to access the QGW series via Samba (Microsoft Networking). Both the local QGW users and LDAP users can access the QGW series via the following protocols/services:
  - AFP
  - FTP
  - File Station

## Joining QGW to Active Directory (Windows Server 2003/2008/2012)

Active Directory is a directory used in Windows environments to centrally store, share, and manage a network's information and resources. It is a hierarchical data centre which centrally holds information for users, user groups, and the computers for secure access management. The QGW series supports Active Directory (AD.) By joining the QGW series to the Active Directory, all the user accounts of the AD server will be automatically imported to the QGW series. AD users can use their same login details to access the QGW series. If you are using Active Directory with Windows Server 2008 R2, you must update the QGW series firmware to at least 3.2.0 to join the QGW series to the AD.

### Joining the QGW to Active Directory Manually

Follow the steps below to join the QGW series to the Windows Active Directory.

1. Login to the QGW series as an administrator. Go to "System Settings" > "General Settings" > "Time". Set the date and time of the QGW series, which must be consistent with the time of the AD server. The maximum time disparity tolerated is 5 minutes.
2. Go to "System Settings" > "Network" > "TCP/IP". Set the IP of the primary DNS server as the IP of the Active Directory server that contains the DNS service. It must be the IP of the DNS server that is used for your Active Directory. If you use an external DNS server, you will not be able to join the domain.
3. Go to "Privilege Settings" > "Domain Security". Enable "Active Directory authentication (domain member)", and enter the AD domain information.

#### Note:

- Enter a fully qualified AD domain name, for example, qnap-test.com
- The AD user entered here must have administrator access rights to the AD domain.
- WINS Support: If you are using a WINS server on the network and the workstation is configured to use that WINS server for name resolution, you must set up the WINS server IP on the QGW series (use the specified WINS server.)

### Joining the QGW to Active Directory (AD) by Quick Configuration Wizard

To join the QGW series to an AD domain by the Quick Configuration Wizard, follow these steps:

1. Go to "Privilege Settings" > "Domain Security". Select "Active Directory authentication (domain member)" and click "Quick Configuration Wizard".
2. Read the wizard introduction. Click "Next".
3. Enter the domain name of the domain name service (DNS.) The NetBIOS name will be automatically generated when you enter the domain name. Specify the DNS server IP for

domain resolution. The IP must be the same as the DNS server of your Active Directory. Click "Next".

4. Select a domain controller from the drop-down menu. The domain controller is responsible for time synchronization between the QGW series and the domain server and user authentication. Enter the domain administrator name and password. Click "Join".
5. Upon successful login to the domain server, the QGW series has joined to the domain. Click "Finish" to exit the wizard.
6. Go to "Privilege Settings" > "Users" or "User Groups" to load the domain users or user groups to the QGW series.

### **Windows 2003**

The AD server name and AD domain name can be checked in "System Properties" in Windows. As an example, for Windows 2003 servers, if you see "node1.qnap-test.com" as the "Full computer name" on the system properties dialog window, the AD server name is "node1" and NOT "node1.qnap-test.com" and the domain name remains the same as qnap-test.com.

### **Windows Server 2008**

Check the AD server name and domain name in "Control Panel" > "System" in Windows. In the system dialog window, the AD server name will appear as the computer name and the domain name can be found in the domain field.

#### **Note:**

After joining the QGW series to the Active Directory, the local QGW users who have access rights to the AD server should use "QGW system name\username" to login. AD users should use their own usernames to login to the AD server.

### **Verifying the settings**

To verify that the QGW series has successfully joined the Active Directory, go to "Privilege Settings" > "Users" and "User Groups". A list of users and user groups will be shown on the "Domain Users" and "Domain Groups" lists respectively. If you have created new users or user groups in the domain, you can click the reload button to add users and user group lists from the Active Directory to the QGW series. The user permission settings will be synchronized in real time with the domain controller.

# Connecting QGW to an LDAP Directory

LDAP (Lightweight Directory Access Protocol) is a directory that can store the information of every user and group in a centralized server. Administrators can use LDAP to manage users in the LDAP directory and allow them to connect to multiple QGW systems with the same login details. This feature is intended for use by administrators and users who have knowledge of Linux servers, LDAP servers, and Samba. A running LDAP server is required when using this feature.

## Requirements

Required information/settings:

- The LDAP server connection and authentication information
- The LDAP structure, where the users and groups are stored
- The LDAP server security settings

## Connecting QGW System to LDAP Directory

Follow the steps below to connect the QGW series to an LDAP directory:

1. Login to the QGW series as an administrator.
2. Go to "Privilege Settings" > "Domain Security". By default, "No domain security" is enabled. This means only local QGW users can connect to the QGW series.
3. Select "LDAP authentication" and complete the settings.
  - LDAP Server Host: The host name or IP address of the LDAP server.
  - LDAP Security: Specify how the QGW series will communicate with the LDAP server:
    - ldap:// = Use a standard LDAP connection (default port: 389.)
    - ldap:// (ldap + SSL) = Use an encrypted connection with SSL (default port: 686.) This is normally used by older version of LDAP servers.
    - ldap:// (ldap + TLS) = Use an encrypted connection with TLS (default port: 389.) This is normally used by newer version of LDAP servers
  - BASE DN: The LDAP domain. For example: dc=mydomain,dc=local
  - Root DN: The LDAP root user. For example cn=admin, dc=mydomain,dc=local
  - Password: The root user password.
  - Users Base DN: The organization unit (OU) where users are stored. For example: ou=people,dc=mydomain,dc=local
  - Groups Base DN: The organization unit (OU) where groups are stored. For example ou=group,dc=mydomain,dc=local
4. Click "Apply" to save the settings. Upon successful configuration, the QGW series will be able to connect to the LDAP server.

## 5. Configure LDAP authentication options.

- If Microsoft Networking has been enabled (Network Services > Win/Mac/NFS > Microsoft Networking) when applying the LDAP settings, specify the users who can access the QGW series via Microsoft Networking (Samba.)
  - Local users only: Only local QGW users can access the QGW series via Microsoft Networking.
  - LDAP users only: Only LDAP users can access the QGW series via Microsoft Networking.
- If Microsoft Networking is enabled after the QGW series has already been connected to the LDAP server, select the authentication type for Microsoft Networking.
  - Standalone Server: Only local QGW users can access the QGW series via Microsoft Networking.
  - LDAP Domain Authentication: Only LDAP users can access the QGW series via Microsoft Networking.

## 6. When the QGW series is connected to an LDAP server, the administrator can:

- Go to "Privilege Settings" > "Users" and select "Domain Users" from the drop-down menu. The LDAP users list will be shown.
- Go to "Privilege Settings" > "User Groups" and select "Domain Groups" from the drop-down menu. The LDAP groups will be shown.
- Specify the folder permissions of LDAP domain users or groups in "Privilege Settings" > "Shared Folders" > click the "Access Permissions" button next to the folder to be configured.

**Note:** Both LDAP users and local QGW users can access the QGW series via File Station, FTP, and AFP.

## LDAP Authentication Technical Requirements with Microsoft Networking

Required items to authenticate the LDAP users on Microsoft Networking (Samba):

1. A third-party software to synchronize the password between LDAP and Samba in the LDAP server.
2. Importing the Samba schema to the LDAP directory.

### A. Third-party software

Some software applications are available and allow management of LDAP users, including Samba password. For example:

- LDAP Account Manager (LAM), with a web-based interface, available from: <http://www.ldap-account-manager.org/>
- smbldap-tools (command line tool)
- webmin-ldap-useradmin - LDAP user administration module for Webmin.

## B. Samba schema

To import a Samba schema to the LDAP server, please refer to the documentation or FAQ of the LDAP server. A samba.schema file is required and can be found in the directory examples/LDAP in the Samba source distribution. Example for open-ldap in the Linux server where the LDAP server is running (it can be different depending on the Linux distribution):

Copy the samba schema:

```
zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz >
/etc/ldap/schema/samba.schema
```

Edit /etc/ldap/slapd.conf (openldap server configuration file) and make sure the following lines are present in the file:

```
include /etc/ldap/schema/samba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/nis.schema
```

## Configuration examples

The following are some configuration examples. They are not mandatory and need to be adapted to match the LDAP server configuration:

### 1. Linux OpenLDAP Server

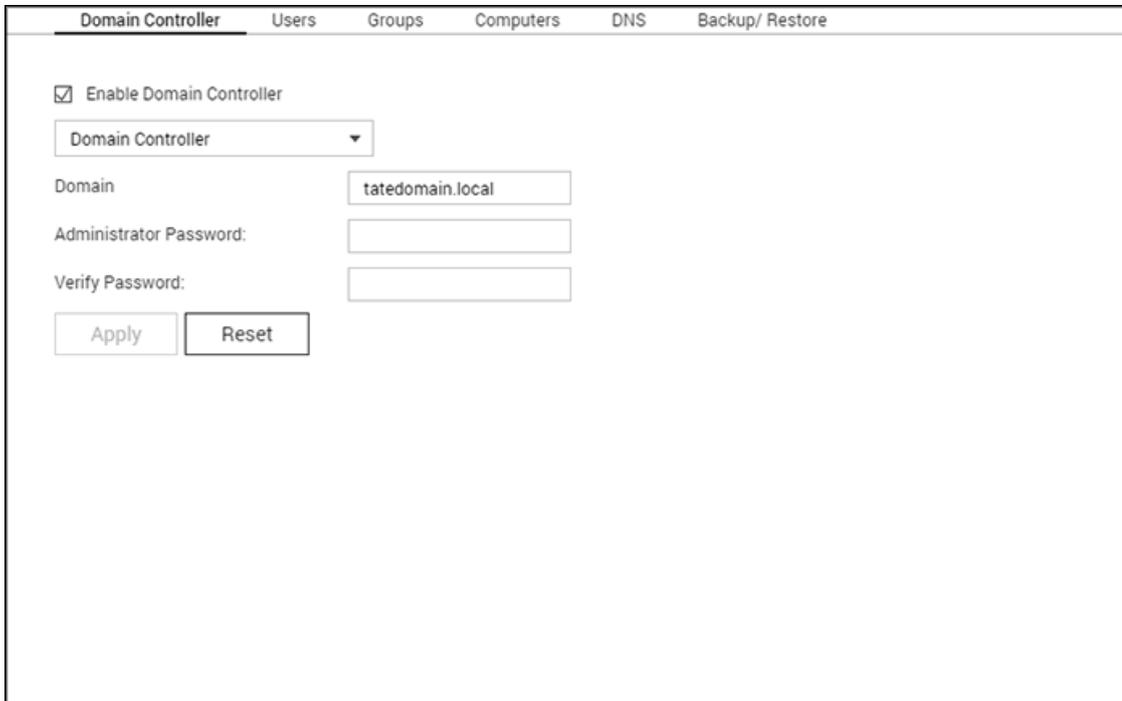
- Base DN: dc=qnap,dc=com
- Root DN: cn=admin,dc=qnap,dc=com
- Users Base DN: ou=people,dc=qnap,dc=com
- Groups Base DN: ou=group,dc=qnap,dc=com

### 2. Mac Open Directory Server

- Base DN: dc=macserver,dc=qnap,dc=com
- Root DN: uid=root,cn=users,dc=macserver,dc=qnap,dc=com
- Users Base DN: cn=users,dc=macserver,dc=qnap,dc=com
- Groups Base DN: cn=groups,dc=macserver,dc=qnap,dc=com

# Domain Controller

The QGW series can now act as a domain controller for Windows. IT administrators can easily configure the QGW series as the centerpiece of domain directory services for their organization to store user account information, manage user authentication and enforce security for a Windows domain.



The screenshot shows a configuration window with a tabbed interface. The 'Domain Controller' tab is selected. The window contains the following elements:

- A checked checkbox labeled 'Enable Domain Controller'.
- A dropdown menu currently set to 'Domain Controller'.
- A text input field for 'Domain' containing the value 'tatedomain.local'.
- A text input field for 'Administrator Password'.
- A text input field for 'Verify Password'.
- Two buttons at the bottom: 'Apply' and 'Reset'.

**Note:** This function is only applicable to some models.

## Domain Controller

Three domain controller modes are available for the QGW series:

- **Domain Controller:** Only a domain controller can create a domain and the first QGW system that creates the domain must be a domain controller. In this mode, the QGW series can create and authenticate users.
- **Additional Domain Controller:** In case more than one domain controller is needed, you can choose this mode to add additional domain controllers. The QGW series set as an additional domain controller will then act as a domain controller and can create and authenticate users.
- **Read-Only Domain Controller:** To accelerate the user authentication process on specific sites, it is possible to enable a Read-Only domain controller. Users can be authenticated by this QGW series, but it will not be able to create a domain user.

To set the QGW series as a domain controller, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Domain Controller" tab.

2. Select a domain controller mode from the drop down list.
3. Specify a domain (example: mydomain.mycompany.local.)
4. Fill out the administrator password and the same password again in the "Verify Password" field.
5. Click "Apply".

After a domain controller is enabled, only the domain users can connect to Microsoft Networking shared folders. Please be sure to grant shared folder permissions to domain users and groups.

**Note:** The QGW series can only act as either a domain controller or LDAP server. If the option "Enable Domain Controller" is grayed out, please disable the LDAP Server in "Control Panel" > "Applications" > "LDAP Server" first.

## Users

You can create or delete domain user accounts or manage their membership here.

### Creating a user

To create a domain user, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.
2. Click "Create" > "Create a User".
3. Follow the instructions of the wizard to complete the details.

### Creating multiple users

To create multiple domain users, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.
2. Click "Create" > "Create Multiple Users".
3. Click "Next".
4. Enter the name prefix, e.g. test. Enter the start number for the username, e.g. 0001 and the number of users to be created, e.g. 10. The QGW series creates ten users named test0001, test0002, test0003...test0010. The password entered here is the same for all the new users.
5. Select to create a private shared folder for each user or not. The shared folder will be named after the username. If a shared folder of the same name has already existed, the QGW series will not create the folder.
6. Specify the folder settings.
7. You can view the new users created in the last step. Click "Finish" to exit the wizard.
8. Check that the users have been created.
9. Check that the shared folders have been created for the users.

## Batch importing users

To batch import domain users, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users" tab.
2. Click "Create" > "Batch Import Users".
3. Select the option "Overwrite existing users" to overwrite existing domain users (or leave this option unchecked if you want to import domain users without overwriting exist ones.) Click "Browse" and select a CSV file which contains the user information in the following format (account, password, description and email.) For steps to create a CSV file, refer to the next section **Creating a CSV File (Excel)**.
4. Click "Next" to import the users and "Finish" after the users have been created.
5. The imported user accounts will be shown.

### Note:

- The password rules (if applicable) will not be applied when importing the users.
- The account and password fields can not be empty for an account.

## Creating a CSV file (Excel)

1. Open a new file with Excel.
2. Enter an user's information in the same row in the following order:
  - Column A: Account
  - Column B: Password
  - Column C: Description
  - Column D: Email
3. Go to the next row and repeat the previous step to create another user account. Each row indicates one user's information. Save the file in CSV format.
4. Open the CSV file with Notepad and save it in UTF-8 encoding if it contains double-byte characters.

## Deleting users

To delete a domain user account, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Users".
2. Select the user account(s) to be deleted.
3. Click "Delete".
4. Click "Yes".

## User account management

Refer to the following table for available buttons under "Action" and their explanations:

Button	Name	Description
	Edit Password	Edit the password of a domain user account.
	Edit User Properties	Specify whether the domain user must change the password at the first login, account expiration date, description and email.
	Edit Group Membership	Choose which domain group(s) the domain user belongs to.
	Edit User Profile	Specify the profile path, login script, and home folder of a domain user account.

For user profiles:

- Profile path: Specify the shared folder where the roaming profiles are stored. The path specified can be a shared folder name such as /home or /user1profile, or a UNC path such as \\nas.mydomain.local\home.
- Login script: Specify the logon script to execute when a domain user logs on from a PC member of the domain. Copy the script to the shared folder (sysvol) in the subfolder {your\_domain}\scripts by connecting to the share \\QGW\netlogon with the domain administrator, and then you can directly specify the script filename.
- Home: Specify the drive letter and a shared folder that is mapped to the drive letter when the domain user logs on to the domain with the domain username and password. The path specified can be a shared folder name such as /home or /user1profile, or a UNC path such as \\nas.mydomain.local\home.

## Groups

To enhance security control, you can create domain user groups. A domain user group is a collection of domain users who share the same access rights to files and folders.

### Creating domain user groups

To create a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Click "Create a User Group".
3. Select "Yes" and "Next" to assign domain user(s) to the group or "No" to create a domain group without domain users.
4. Click "Finish".

## Deleting domain user groups

To delete a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Select user group(s) and click "Delete".

**Note:** It is advised not to delete the default existing group of the domain.

## Editing group members

To edit domain members within a group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Click the "Edit Group Membership" button under "Action".
3. Select and check domain users to join them to the group or uncheck existing domain users to remove them from the group.
4. Click "Next".

## Computers

All computers that have already joined the domain will be listed here, and with permissions granted, they can access the list of domain resources (such as the domain users and groups.) The computer accounts are created automatically after the computers or the QGW system joins the domain, and administrators can manually create or delete computer accounts.

## Creating computer accounts

To create a domain computer account, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Computers" tab.
2. Click "Create a Computer".
3. Fill out the computer name, description and location and click "Next".
4. Choose the group(s) for the computer account and click "Next".
5. Click "Create".

## Deleting computer accounts

To delete a domain user group, follow the steps below:

1. Go to "Control Panel" > "Privilege Settings" > "Domain Controller" > "Groups" tab.
2. Select the computer account(s) and click "Delete".
3. Click "Delete".

## Computer account management

Refer to the following table for available buttons under "Action" and their explanations:

Button	Name	Description
	Edit Computer Properties	Edit the description and location of the computer account.
	Edit Group Membership	Choose to add the computer account to the user group(s) or remove it from the user group(s).

## DNS

The Domain Name System, or DNS, can help the domain controller locate services and devices within the domain (or vice versa) using service and resource records. Two DNS zones are created by default (the domain created when you first set up the QGW series as the domain controller and the zone with a name starting with \_msdcs.) System administrators can modify DNS settings, add/delete domains, and add/delete records.

### Modifying DNS settings

To edit a DNS setting, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password, and the DNS settings will appear.

Follow the steps below:

1. Click the setting to be modified
2. Edit the properties of the setting (type and value), adjust the order of the value with the green up-arrow or down-arrow button, or delete the value with the red "X" button.
3. Click "Apply" to save the changes.

### Adding domains

To add a domain, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Click "Action" > "Add Domain".
2. Enter the domain name and click "Create".

### Adding records

To add a record, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Select a domain
2. Click "Action" > "Add Record".
3. Enter the record properties and click "Create".

**Note:** Only the following types of records are supported: A, AAAA, PTR, CNAME, NS, MX, SRV, TXT.

### **Deleting domains or records**

To delete a record, first go to "Control Panel", Privilege Settings" > "Domain Controller" > "DNS tab" and log in with the administrator username and password. Follow the steps below:

1. Select a domain or record
2. Click "Action" > "Delete".
3. Click "Yes".

### **Backup/Restore**

The domain controller status can be backed up or restored using the backup/restore function. Only the first domain controller needs to be backed up. In an AD environment where more than one domain controller presents, there are some restrictions and limitations associated with the restore procedures. Please check the restore function carefully.

### **Backing up domain controllers**

To back up the domain controller status, follow the steps below:

1. Go to "Control Panel", Privilege Settings" > "Domain Controller" > "Backup/Restore tab"
2. Check "Back up Database" and set the backup frequency, starting time, destination folder and backup options (choose to overwrite existing backup file or create a new file.)
3. Click "Apply"

### **Restoring domain controllers**

Please note that the current settings, including users, groups and domain controller settings, will be overwritten and all changes made since the last backup will be lost. So, please be specially careful when you restore domain controllers.

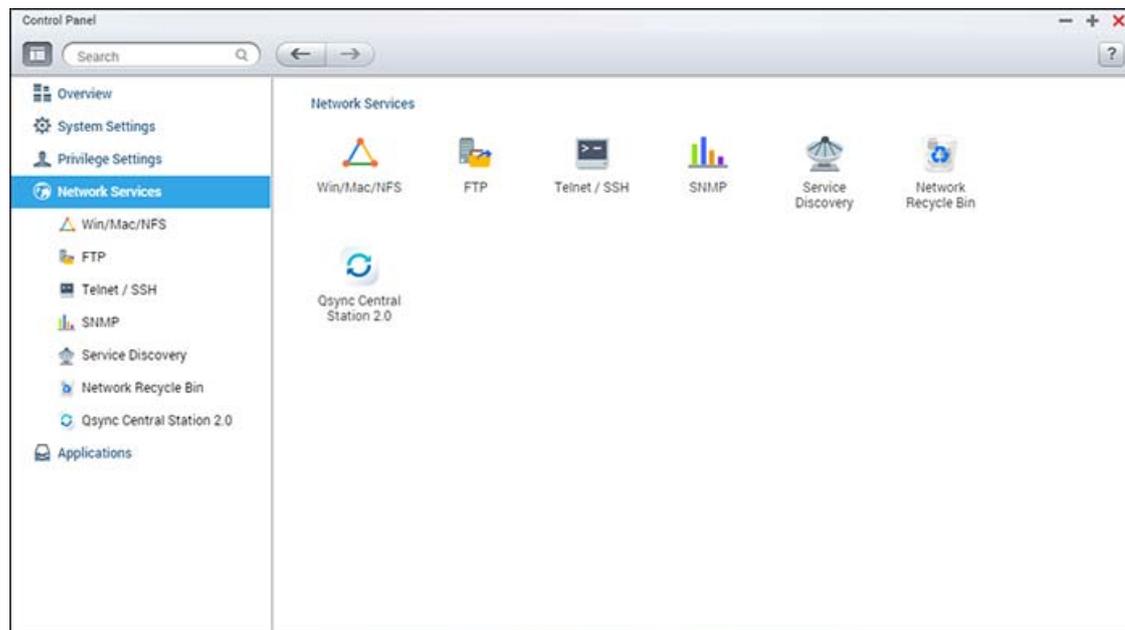
To restore the domain controller in a single domain controller environment, follow the steps below:

1. Go to "Control Panel", Privilege Settings" > "Domain Controller" > "Backup/Restore tab" > scroll down to the "Restore ADDC Database" section.
2. Click "Browse" and select the backup file.
3. Click "Import".

If the domain controller you try to restore is in an environment with more than one domain controllers, do not restore from the backup, as this will corrupt the domain controller database. Simply add the QGW system back as a domain controller, and it will synchronize with the existing domain controller. If no other domain controllers are online, restore only the first domain controller, and join the other QGW system as the domain controller back. To restore a domain to a previous state with multiple domain controllers, first disable the domain controller feature on all QGW systems, restore only the first domain controller, and join the other QGW systems as domain controller back.

# Network Services

Go to "Control Panel" > "Network Services" to configure network services on the QGW series.



For setup details, refer to the following links:

- [Win/Mac/NFS](#)
- [FTP](#)
- [Telnet/SSH](#)
- [SNMP Settings](#)
- [Service Discovery](#)
- [Network Recycle Bin](#)
- [Qsync Central Station](#)

# Win/Mac/NFS

Go to "Control Panel" > "Network Services" > "Win/Mac/NFS" to configure networking services.

Microsoft Networking Apple Networking NFS Service

Enable file service for Microsoft networking

Server description (Optional):

Workgroup:

Standalone server

AD domain member (To enable Domain Security, please click here.)

LDAP domain authentication (To enable Domain Security, please click here.)

Current Samba ID: --

Advanced Options

Apply

Apply All

In this chapter, the following topics are covered:

- [Microsoft Networking](#)
- [Apple Networking](#)
- [NFS Service](#)

## Microsoft Networking

To allow access to the QGW system on Microsoft Windows Network, enable file service for Microsoft networking. Also specify how users will be authenticated.

### Standalone Server

Use local users for authentication. The QGW series will use local user account information (created in "Privilege Settings" > "Users") to authenticate users who access the QGW series.

- Server Description (optional): Describe the QGW series so that users can easily identify it on a Microsoft Network.
- Workgroup: Specify the workgroup to which the QGW series belongs. A workgroup name supports up to 15 characters but cannot contain: " + = / \ : | \* ? < > ; [ ] % , `

## AD Domain Member

Use Microsoft Active Directory (AD) to authenticate users. To use this option, enable Active Directory authentication in "Privilege Settings" > "Domain Security" and join the QGW series to an Active Directory.

## LDAP Domain Authentication

Use an LDAP directory to authenticate the users. To use this option, enable LDAP authentication and specify the settings in "Privilege Settings" > "Domain Security". When this option is enabled, you need to select either the local QGW users or the LDAP users that can access the QGW series via Microsoft Networking.

## Advanced Options

- **WINS server:** If you have a WINS server on your network and want to use this server, enter the WINS server IP. The QGW series will automatically register its name and IP address with the WINS service. Do not enable this option if you are unsure about the settings.
- **Local Domain Master:** A Domain Master Browser is responsible for collecting and recording resources and services available for each PC on the network or a workgroup of Windows. When you find the waiting time for loading network resources to be too long, it may be caused by a failure of an existing master browser or a missing master browser on the network. If there is no master browser on your network, select the option "Domain Master" to configure the QGW series as the master browser. Do not enable this option if you are unsure about the settings.
- **Allow only NTLMv2 authentication:** NTLMv2 stands for NT LAN Manager version 2. When this option is enabled, login to the shared folders by Microsoft Networking will only be allowed using NTLMv2 authentication. If the option is disabled, NTLM (NT LAN Manager) will be used by default and NTLMv2 can be negotiated by the client. The default setting is disabled.
- **Name resolution priority:** You can select to use DNS server or WINS server to resolve client host names from IP addresses. When you set up your QGW system to use a WINS server or to be a WINS server, you can choose to use DNS or WINS first for name resolution. When WINS is enabled, the default setting is "Try WINS then DNS". Otherwise, DNS will be used for name resolution by default.
- **Login style: DOMAIN\USERNAME instead of DOMAIN+USERNAME for FTP, AFP, and File Station:** In an Active Directory environment, the default login formats for the domain users are:
  - Windows shares: domain\username
  - FTP: domain+username
  - File Station: domain+username

- AFP: domain+username

When you enable this option, users can use the same login name format (domain\username) to connect to the QGW series via AFP, FTP, and File Station.

- **Automatically register in DNS:** When this option is enabled and the QGW series is joined to an Active Directory, the QGW series will automatically register itself in the domain DNS server. This will create a DNS host entry for the QGW series in the DNS server. If the QGW IP changes, the QGW series will automatically update the IP in the DNS server.
- **Enable trusted domains:** Select this option to load users from trusted Active Directory domains and specify their QGW **access** permissions in "Privilege Settings" > "Shared Folders". Domain trusts are only set up in Active Directory, not on the QGW system.)

## Apple Networking

To connect to the QGW series from Mac OS X, enable Apple Filing Protocol. If the AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the QGW series. Enter an asterisk (\*) to use default settings. This setting is disabled by default. To allow access to the QGW series from Mac OS X 10.7 Lion, enable "DHX2 authentication support". Click "Apply" to save the settings. You can use the Finder to connect to a shared folder from Mac. Go to "Go" > "Connect to Server", or simply use the default keyboard shortcut "Command+k". Enter the connection information in the "Server Address" field, such as "afp://YOUR\_QGW\_IP\_OR\_HOSTNAME". Here are some examples:

- afp://10.8.12.111
- afp://NAS-559
- smb://192.168.1.159

**Note:** Mac OS X supports both Apple Filing Protocol and Microsoft Networking. To connect to the QGW series via Apple Filing Protocol, the server address should start with "afp://". To connect to the QGW series via Microsoft Networking, please use "smb://".

## NFS Service

To connect to the QGW series from Linux, enable the NFS service. To configure NFS access rights to shared folders on the QGW series, go to "Privilege Settings" > "Share Folders" and click the Access Permission button on the "Action" column. Select NFS host access from the drop-down menu on the top of the page and specify the access rights. If you select "No limit" or "Read only", you can specify the IP address or domains that are allowed to connect to the folder by NFS.

- No limit: Allow users to create, read, write, and delete files or folders in the shared folder and any subdirectories.

- Read only: Allow users to read files in the shared folder and any subdirectories but they are not allowed to write, create, or delete any files.
- Deny access: Deny all access to the shared folder.

### Connecting to the QGW series by NFS

On Linux, run this command:

```
mount -t nfs <QGW system IP>:/<Shared Folder Name> <Directory to Mount>
```

For example, if the IP address of your QGW system is 192.168.0.1 and you want to link the shared folder "public" under the /mnt/pub directory, use this command:

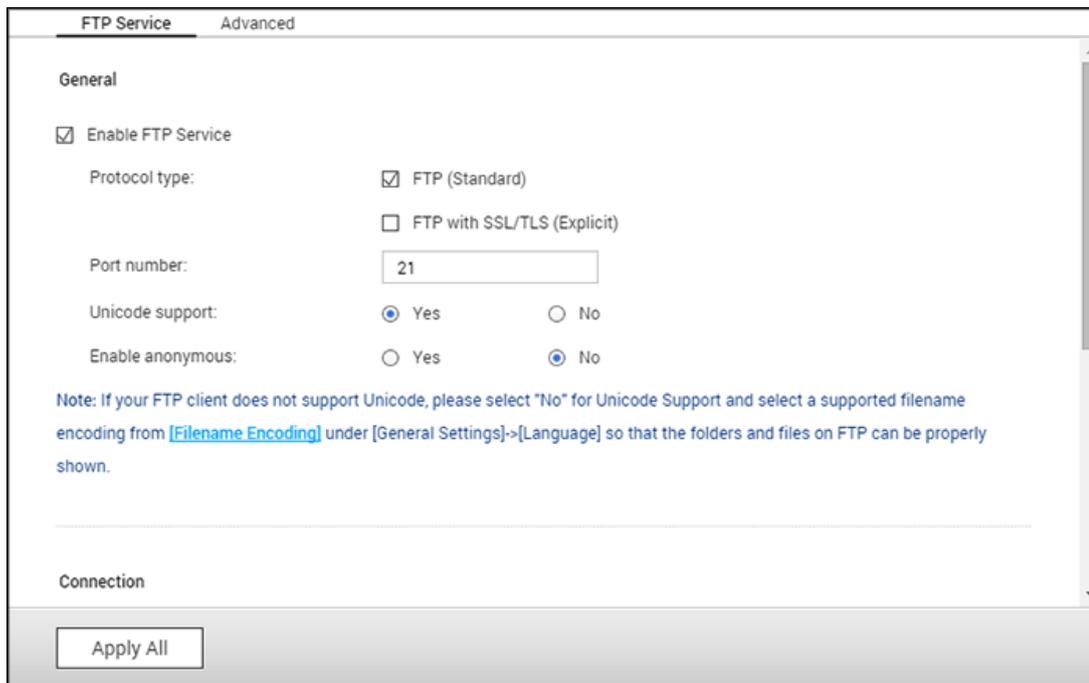
```
mount -t nfs 192.168.0.1:/public /mnt/pub
```

**Note:** You must login as the "root" user to use the above command.

Login as the user ID you define, you can use the mounted directory to connect to your shared files.

# FTP

Go to "Control Panel" > "Network Services" > "FTP" to Configure the FTP server.



## FTP Service

When you enable the FTP service, you can specify the port number and the maximum number of users that are allowed to connect to the QGW series by FTP at the same time. To use the FTP service of the QGW series, enable this function. Open an IE browser and enter ftp://QGW IP. Enter the username and the password to login the FTP service.

- **Protocol Type:** Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the correct protocol type in your client FTP software to ensure successful connection.
- **Port number:** Specify the port number of the FTP service.
- **Unicode Support:** Toggles Unicode support. The default setting is No. If your FTP client does not support Unicode, it is recommended to disable this option and select the specified language in "General Settings" > "Codepage" so that the file and folder names can be correctly displayed. If your FTP client supports Unicode, enable this option for both your client and QGW system.
- **Enable Anonymous:** Enable this option to allow anonymous access to the QGW series by FTP. Anonymous users can connect to files and folders which are open for public access. If this option is disabled, users must enter an authorized username and password to connect to the QGW series.
- **Connection:** Enter the maximum number of allowed FTP connections for the QGW series and a single account and check "Enable FTP transfer limitation" to specify the maximum upload and download rates.

**Note:** The maximum number of FTP connections varies based on the size of RAM installed on the QGW series:

- If the QGW system memory  $\leq$  1 GB, the maximum is 256.
- If the QGW system memory = 2 GB, the maximum is 512.
- If the QGW system memory  $\geq$  3 GB, the maximum is 1024.

## Advanced

- **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 (QGW series) is behind a router, and a remote computer cannot connect to the FTP server over the WAN. When this is enabled, the QGW series 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.

# Telnet/SSH

Enable this option to connect to the QGW series by Telnet or SSH encrypted connection (only the "admin" account can remotely login.) Use Telnet or SSH connection clients, for example, putty for connecting. Make sure the specified ports have been opened on the router or firewall.

After enabling this option, you can access this server via Telnet or SSH connection.

Note: Only the account admin can login remotely.

Allow Telnet connection

Port number:

Allow SSH connection

Port number:

Enable SFTP

To use SFTP (SSH File Transfer Protocol/Secure File Transfer Protocol), make sure the option "Allow SSH connection" has been enabled.

# SNMP Settings

Enable SNMP (Simple Network Management Protocol) on the QGW series and enter the trap address of the SNMP management stations (SNMP manager) - for example, a PC with SNMP software installed. When an event, warning, or error occurs on the QGW series, it will report a real-time alert to SNMP management stations.

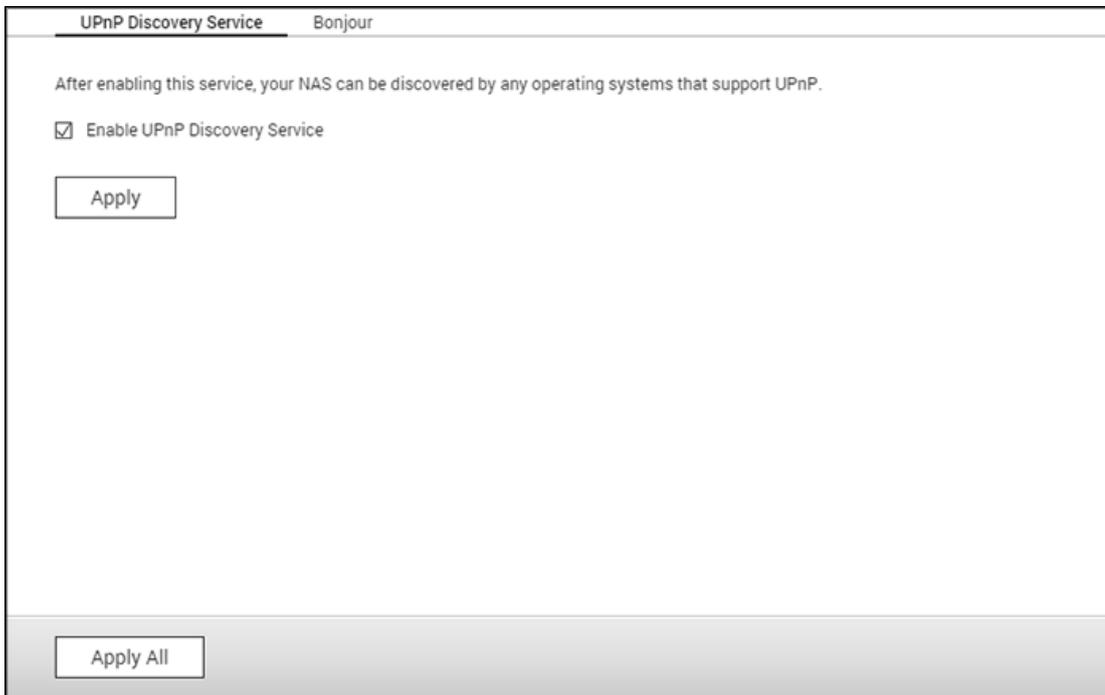
The fields are described as below:

Field	Description
SNMP Trap Level	Select information to be sent to the SNMP management stations.
Trap Address	The IP address of the SNMP manager. Specify up to 3 trap addresses.
SNMP MIB (Management Information Base)	The MIB is a type of database in ASCII text format used to manage the QGW series in the SNMP network. The SNMP manager uses the MIB to determine the values or understand the messages sent from the agent (QGW series) within the network. You can download the MIB and view it with any word processor or text editor.
Community (SNMP V1/V2)	An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the QGW series. The

	community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
SNMP V3	The QGW series supports SNMP version 3. Specify the authentication and privacy settings if available.

# Service Discovery

Go to "Control Panel" > "Network Services" > "Service Discovery" to configure the UPnP discovery service and Bonjour.



The screenshot shows a web interface for configuring network services. At the top, there are two tabs: "UPnP Discovery Service" (which is selected) and "Bonjour". Below the tabs, there is a text box stating: "After enabling this service, your NAS can be discovered by any operating systems that support UPnP." Below this text, there is a checkbox labeled "Enable UPnP Discovery Service" which is checked. Below the checkbox is an "Apply" button. At the bottom of the page, there is a grey bar containing an "Apply All" button.

## UPnP Discovery Service

When a UPnP device is added to the network, the UPnP discovery protocol allows the device to advertise its services to the network control points. By enabling UPnP Discovery Service, the QGW series can be discovered by any systems that support UPnP.

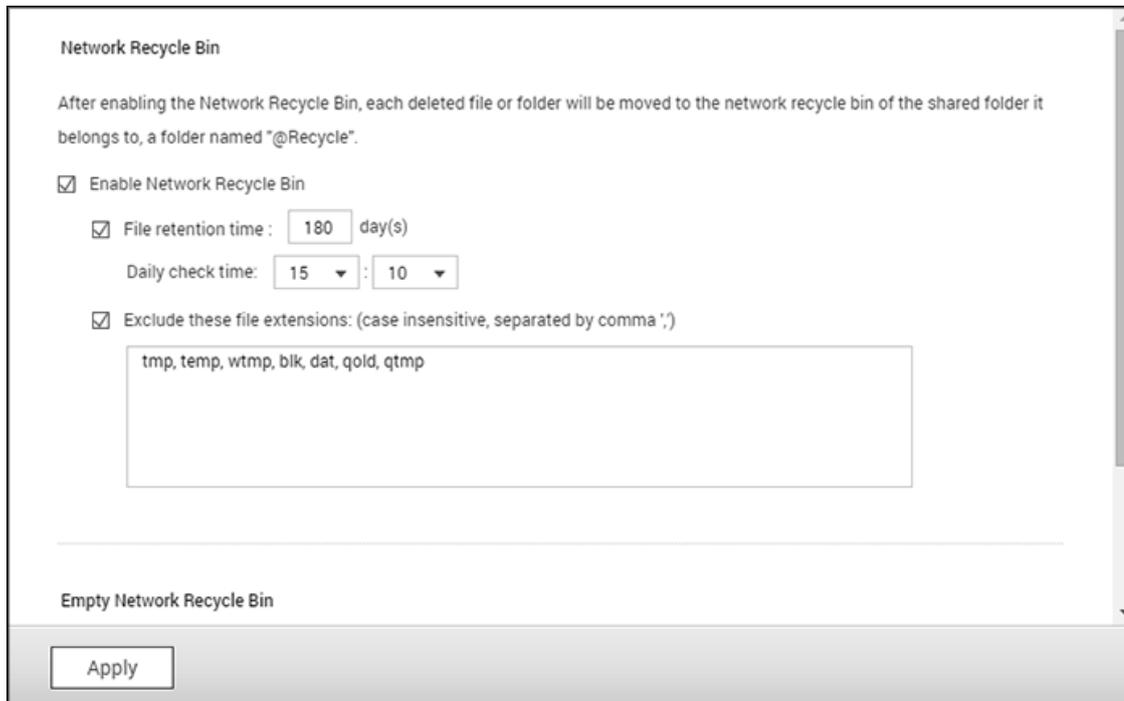
## Bonjour

By using Bonjour, your Mac will automatically discover network services (such as FTP) running on the QGW series without needing to enter IP addresses or configuring DNS servers.

**Note:** You must activate the services on their setup pages and then enable them in this section so that the QGW series can advertise them using Bonjour.

# Network Recycle Bin

The Network Recycle Bin retains files deleted on the QGW series. Within each shared folder, a dedicated folder with the name @Recycle is created after the initial QTS Gateway installation. Specify the number of days (1-180) to retain files and the daily time. You can also specify the file extensions to be excluded from the bin. This feature only supports file deletion via Samba, AFP, FTP and File Station.



The screenshot shows the 'Network Recycle Bin' configuration window. At the top, it explains that after enabling the feature, deleted files are moved to a folder named '@Recycle'. Below this, there are several options: 'Enable Network Recycle Bin' is checked; 'File retention time' is set to 180 days; 'Daily check time' is set to 15:10; and 'Exclude these file extensions' is checked with a text box containing 'tmp, temp, wtmp, blk, dat, qold, qtmp'. At the bottom, there is an 'Empty Network Recycle Bin' button and an 'Apply' button.

## Using Network Recycle Bin

- To delete all the files in the bin, click "Empty All Network Recycle Bin".
- To recover deleted files from the Network Recycle Bin, right click on the files in the @Recycle folder and select "RECOVER".
- To permanently delete a file in the recycle bin, right click on the file in the @Recycle folder and select "Del (from recycle)".
- To empty the recycle bin for an individual shared folder, right click inside the recycle bin and select "Empty Recycle Bin".

## Restricting Access to Network Recycle Bin

The Network Recycle Bin can be restricted to administrators usage by going to "Control Panel" > "Privilege Settings" > "Shared Folders". Click "Property" under "Action" for the shared folder to be configured and check "Restrict the access of Recycle Bin to administrators only for now".

**Caution:** All of the files in network recycle bins will be permanently deleted when files are deleted in "@Recycle" on the network share or when you click "Empty All Network Recycle Bins". The Network Recycle Bin feature is not supported for USB external storage devices and virtual disks.

# Qsync Central Station

Qsync Central Station 2.0 is a cloud-based file synchronization service on the QGW series. Simply add files to your local Qsync folder, and they will be available on your QGW series and all its connected devices.



In this chapter, the following topics are covered:

- [Before you Start](#)
- [Starting Qsync Client](#)
- [Synchronization](#)
- [Sharing](#)
- [Remote Access](#)
- [Synchronization Management](#)
- [Version Control](#)
- [Managing or Monitoring Qsync Status via Web Browser](#)
- [Using Centralized Mode for Centralized Management](#)

## Before you Start

Follow the 3 steps below before Qsync deployment.

1. Creating user accounts on the QGW series,
2. Downloading the Qsync Client utility on your computers and Qfile on your mobile devices,
3. Logging into the QGW series (serving as a Qsync server) from your computers or mobile devices (referred to in this document as "Qsync clients".)

### 1. Creating user accounts on the QGW series

- Go to "Control Panel" > "Privilege Settings" > "Users" > click "Create" (or go to "Qsync Central Station 2.0" > "Users" > "Create a User".)
- Only QGW administrators can create accounts.

## 2. Downloading Qsync Client

Follow the instructions on the "Overview" page to download the utility (log into the QGW series > click "Qsync Central Station 2.0" on the QGW Desktop > "Overview" page,) or directly download the utility from the QNAP website: "Support" > "Download" > "Utilities".

- For computers, download the Qsync Client utility (only available for Windows.)
- For mobile devices, download and install Qfile from the iOS or Android app stores.

## 3. Setting up Qsync Client

Launch the installer and follow these steps to set up the Qsync Client:

1. To locate the QGW series within a LAN, simply click "Search" or key in its IP address or name (e.g. IP address: 10.8.1.20 or 192.168.1.100.) To connect to a remote QGW system (over the Internet) use your myQNAPcloud address (e.g. andy@myQNAPcloud.com.)
2. Enter the QGW system login username and password.
3. Set up the Qsync local folder on your PC.
4. Assign a name to identify the local PC for the Qsync server.
5. Click "Apply" .
6. Pair a local folder with the shared folder on the QGW series.

**Note:** If the QGW system connection ports have been changed, please append the port number to the IP address; otherwise only enter an IP address. (Default port number: 8080)

## Starting Qsync Client

Double click the Qsync shortcut in Windows to open the Qsync local folder. Click the Qsync Client icon on the taskbar to bring up the menu. If you copy/move files to the local Qsync folder on one of your devices, the files will be synced with all the other devices (devices with the Qsync Client installed that are connected to the QGW series.) From now on, there is no need to copy files back-and-forth between your PC and these other devices or worry about the size of files as you try to attach them to an email.

## Synchronization

There are several methods for synchronizing files. Qsync Central Station will automatically synchronize the files across your computers and mobile devices that have the Qsync Client installed, and they will also be synchronized to the Qsync folder on the QGW series:

1. For PCs, drag and drop files to the local Qsync folder.
2. For mobile devices (Qfile), copy or move files into the local Qsync folder.

3. For the QGW series, copy or move files to the Qsync folder using File Station.

**Note:**

- If files are "dragged and dropped" to the local Qsync folder, they will be moved (and not copied) to that folder if the files and the local Qsync folder are on the same disk drive. This behavior is the same as Windows File Explorer.
- The maximum size of a single file that Qsync can transmit across a LAN is 50GB.
- Qsync does not support SAMBA, FTP or AFP for files access. Please access files using File Station or a Qsync Client.
- Qfile only synchronizes the file list and does not download the files to a mobile device. Please download the files when you need them.

**Offline editing**

You can edit your files offline and Qsync Central Station will automatically synchronize the changes made once your device is online.

**Sharing**

**Sharing files by download links**

You can share files by sending download links to those who have not installed Qsync Client.

For Windows:

1. Right click on the file that you want to share in the local Qsync folder and click "Share the link".
2. Choose to send the link via email or copy the link to directly share it.
3. Click "Settings" to see more options, including creating a SSL link, the expiration date, or password.

For the QGW series, right click on the file that you want to share in the Qsync folder within File Station and click "Share".

For mobile devices, launch Qfile to share the file in the local Qsync folder by clicking the icon to the right and click "Share".

The file recipients can click the link or copy and paste it to a web browser to download the file.

**Sharing folders with a group**

You can share a folder with a user group. If any member from the group shares the files in the folder, other members can receive the file.

1. Create user accounts in the QGW series for each group member.

2. Ensure that a Qsync Client is installed on each member's device.
3. Right click on the folder you want to share in the local Qsync folder and click "Share this folder as a team folder".
4. Select users from the list of local or domain users.

All of the members in the group will receive a file sharing invitation. Once accepted, the group members can start accessing this shared folder.

**Note:**

- The team folder will only take effect after users accept their invitation.
- Users cannot share team folders that have been shared with them.
- Only the folders under /home on your QGW system can be shared as a Team Folder.

## Remote Access

### Accessing the QGW series over the Internet

To connect to a remote QGW system (over the Internet), the administrator must first configure the device name for the QGW system in "myQNAPcloud". The administrator can then share the myQNAPcloud address to allow users to access the remote QGW system. (e.g. andy@myQNAPcloud.com)

**Note:**

- A connection with a QGW system over the Internet will be slower compared to a LAN environment.
- As you switch back to a LAN-based QGW system, ensure that you reconnect to the QGW system via LAN to get a better connection quality.
- To improve file transmission performance, it is recommended that you configure port forwarding on the router.

### Synchronizing photos and videos automatically

Qsync Central Station can synchronize your photos and videos from mobile devices to the Qsync folder across all Qsync client devices.

Steps:

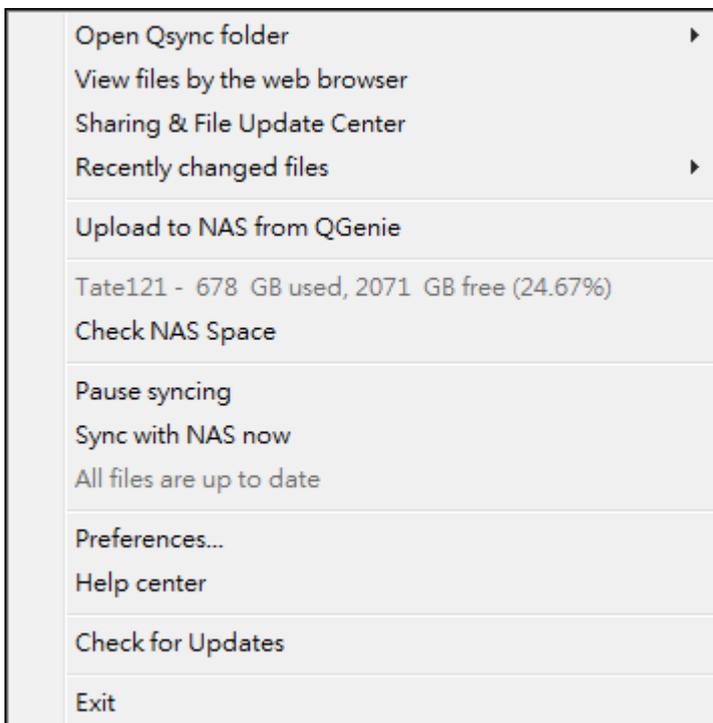
1. Install Qfile on your mobile devices by following instructions outlined on the Qsync Central Station Overview page on the QGW system or find it from your device's app store.
2. Launch Qfile.
3. Click "Settings" on the bottom-right side of the screen.
4. Scroll down and look for "Auto upload from photo gallery" and click on "Set up now".

5. Select a QGW system to upload photos and videos to.
6. Select the folder.
7. Select "Use default setting" ( /Qsync/Camera Uploads) or select "Set up manually" to set the path.
8. Select if you want to upload all photos from the photo gallery immediately.
9. You can tick the checkbox "Limit to Wi-Fi" to ensure that you only upload files through Wi-Fi and not your phone's network.
10. The uploaded files will be synchronized to the "Camera Uploads" folder under the Qsync folder on Qsync client devices.

**Note:** If files that were previously uploaded are deleted from the "Camera Uploads" folder, Qfile will not upload those copies in the photo library again.

## Synchronization Management

Click the Qsync Client icon on the taskbar to see the management functions:



1. Add files and view the synchronization result on the QGW series:
  - a. Open Qsync folder: Open the local Qsync folder to add files.
  - b. View files by the web browser: Browse files in the Qsync folder using File Station.
2. Control synchronization progress:

- a. Pause syncing / Resume syncing: Click to pause or resume syncing.
  - b. Sync with QGW series now: Force Qsync to scan again and refresh the synchronization list.
3. Information for syncing and sharing:
- a. Sharing & File Update Center
    - i. File Update Center: List the file or folder update logs.
    - ii. Sharing Center: List the folders or files shared with others. Users can choose to accept or decline the team folders. However, users cannot share team folders that are shared by others.
  - b. Recently changed files: Lists the recently updated files.
4. Preference:
- a. General:
    - i. Link Status: Shows the current status. Click "Logout" to change users.
    - ii. Network Recycle Bin: Browse or recover files deleted from the Qsync folder.
  - b. Sync:
    - i. Manage paired folders: Add, delete, or edit folder pair settings.
    - ii. Import photos and videos: Import photos and videos when an USB device is connected. This feature only checks for photos and videos in the "DCIM" folder in the root directory of USB devices.
    - iii. Default folder: choose a folder to import files from external drives or QGenie.
    - iv. Do not remove any files on the QGW series when synchronizing: You can remove files within the local Qsync folder, and files deleted from your computer will not be synchronized with the QGW series. The QGW series will still retain copies of deleted files.
  - c. Policy:
    - i. Conflict Policies: The policies for handling the name conflicts between the Qsync server (QGW system) and clients after it is back online from a disconnection:
      - 1) Rename the local files,
      - 2) Rename the remote QGW system files,
      - 3) Replace local files with remote QGW system files, or
      - 4) Replace remote QGW system files with local files.
    - ii. Sharing Policies: The policies of the team folders when other Qsync users share them to this local computer:
      - 1) Always reject sharing,
      - 2) Automatically accept sharing, or
      - 3) Send a notification message once sharing occurs.
    - iii. Filter Settings: During file synchronization, Qsync will skip the file types specified in filter settings.
  - d. E-Mail:

- i. Set up E-mail: Set up an email account for sharing file links. You can use the SMTP server settings (for administrators only), your PC's mail server settings, or configure a new SMTP server.
- e. Proxy:
  - i. Set up Proxy: Use a proxy server for the Qsync client device.
- f. Advanced:
  - i. Debug log: The system will record all of the synchronization activities between your computer and the QGW system for diagnosing technical problems.

**Note:** The "Sync" and "Proxy" tab is not available on Mac.

## Version Control

This will retain one copy of a file as a version whenever you add or modify it, allowing you to retrieve a specific previous version at any time. Or, if you accidentally overwritten a previous version made by others while editing the file in team folder, you can still restore the previous version. And you can restore the previous versions even if you have deleted the file from the recycle bin.

### Viewing the version history

You can view the version history by using File Station. Right click on a file or folder in the Qsync folder in File Station and select "Previous Versions" to show the version list (or you can access it from menu bar "More Action" > "Previous Versions". Or, just click the "Show Right Panel" > "Version". You can also access it from the Qsync client utility. Right click on a file or folder in the Qsync folder and select "Previous Versions".

### Restoring the previous versions

In the version history page, select the version you want to restore and click "Restore".

- Click "Download" to download the version to the local computer.
- Click "Delete All" to delete all of the listed versions.
- Click "Refresh" to update the status of the version history.

### Restoring versions of a deleted file

Version control retains versions in a separate location, so even you delete the file, you can still restore the previous versions of the file - even if the file has been deleted from the recycle bin.

To restore the version of a deleted file, click on any folder/file in the Qsync folder, and then click "More Action" > "Show Deleted Files" in the menu bar. To view the version history, right click on a file/folder in Qsync folder and select "Previous Versions". Or you can access it

from the menu bar, "More Action" > "Previous Versions". Or just click the "Show Right Panel" > "version" to show the version list.

### Restoring previous versions

In the version history page, select the version you want to restore and click "Restore".

- Click "Download" to download the version to the local computer.
- Click "Delete All" to delete all of the listed versions.
- Click "Refresh" to update the status of the version history.

**Note:** If you click "Delete All", then click "Refresh" and the associated files will be removed from the list.

To exit the view of the deleted file list, right click on any file/folder and select "Hide Deleted Files". Or access it from menu bar, "More Action" > "Hide Deleted Files".

### Managing and setting version control

To access the management and settings of version control, click the Qsync button on the desktop of the QGW system, then click "Version Control" in the right-side menu.

#### The target folder

"Enable version control" is the main switch of the version control. Disabling this option will not delete versions that have already been created. "Enable version for my Qsync folder" allows each user to apply the function to their files.

#### Target folder for version control

You can apply the version control to the files under specific Qsync folders to save space. To assign specific folders, select "Assign specific subfolder under the Qsync folder", then click "Add" to add folders. You can add up to 5 folders. Click "Delete" to remove all versions under the selected folders and subfolders. This will not take effect until you click "Apply" or "Apply All".

#### Advanced

**Maximum Number of Versions:** You can choose how many versions you want to retain. This is a control only for administrators. The more versions you keep the more storage space will be taken up. To know how much space has been used for version control, click "Check" in the "Disk Used for Version Control" section.

**Note:**

- If you reduce the maximum number of versions, it will impact the versions that have been created and if the volume of versions exceeds the new settings, the earlier

versions will be dropped. Only the equivalent number of latest versions as of the new settings will be kept.

- The deletion will only take effect after you click "Apply" or "Apply All".
- The maximum number of versions supported for Version Control is 64.

## Managing or Monitoring Qsync Status via Web Browser

Log into the QGW system via web browser and click Qsync Central Station 2.0.

1. Overview: This page shows the mode of use management (User Customization Mode or Central Configuration Mode) and the total number of online users and devices. It also provides links to File Station and for installing Qsync. In addition, you can enable or disable the Qsync service (for administrators only.)
2. Management settings: This provides a centralized management for administrators to edit Qsync Client default settings. For details on the management settings, please refer to the [Using Centralized Mode for Centralized Management](#) section.
3. Users: Lists the information of online users, and you can manage the users of Qsync service here (for administrators only.)
4. Devices: This table lists the status of connected devices. It also provides options for you to manage each device, allowing you to edit their settings, block them, or to remotely erase them.
  - a. If users log in from their PC, the name of the device will be shown as their computer name.
  - b. If users log in from Qfile, the name of the device will be shown as "Qfile-Android" or "Qfile-iPhone".
  - c. If users move or copy files to the Qsync folder in the File Station, the name of the device will be shown as "Qsync-File Station".
5. Event Logs: Lists activity details by user.
6. Team Folder: Lists information about team folders, including folders that you shared and folders that are shared with you.
7. Shared Folder: Administrators can decide which shared folders will be synced with client devices. If a user has Read/Write or Read-only and synchronization privileges on a shared folder, it can then be synced with their client device.
8. Shared File Links: Lists the status of shared links.
9. Version Control: You can set the maximum number of version for your files and check the space used for Version Control.

## Using Centralized Mode for Centralized Management

Administrators can now apply pre-configured settings to devices that connect to the QGW series for the first time, restrict users' right on modifications to all or certain preference settings of their client utilities, edit settings for individual Qsync client devices online, or set a management password (a master password for all client devices.)

To apply pre-configured settings on connected devices, follow these steps:

1. Log into the QGW series as an administrator > "Qsync Central Station 2.0" > Management settings,
2. Click "Edit default settings".
3. Under the "Synchronize" tab, choose whether to remotely remove any files on the QGW series during synchronization.
4. Under the "Policy" tab, set conflict policies, and filter settings.
5. Under the "Mails" tab, set up the email option and sender details.
6. Click "Apply".

To allow all users to configure their own client utility, follow these steps:

1. Log into the QGW series as an administrator > "Qsync Central Station 2.0" > Management settings,
2. Select "Central Configuration Mode" and tick the preference settings that users are allowed to modify for their Qsync client device.
3. Click "Apply".

To edit settings for individual Qsync client devices, follow these steps:

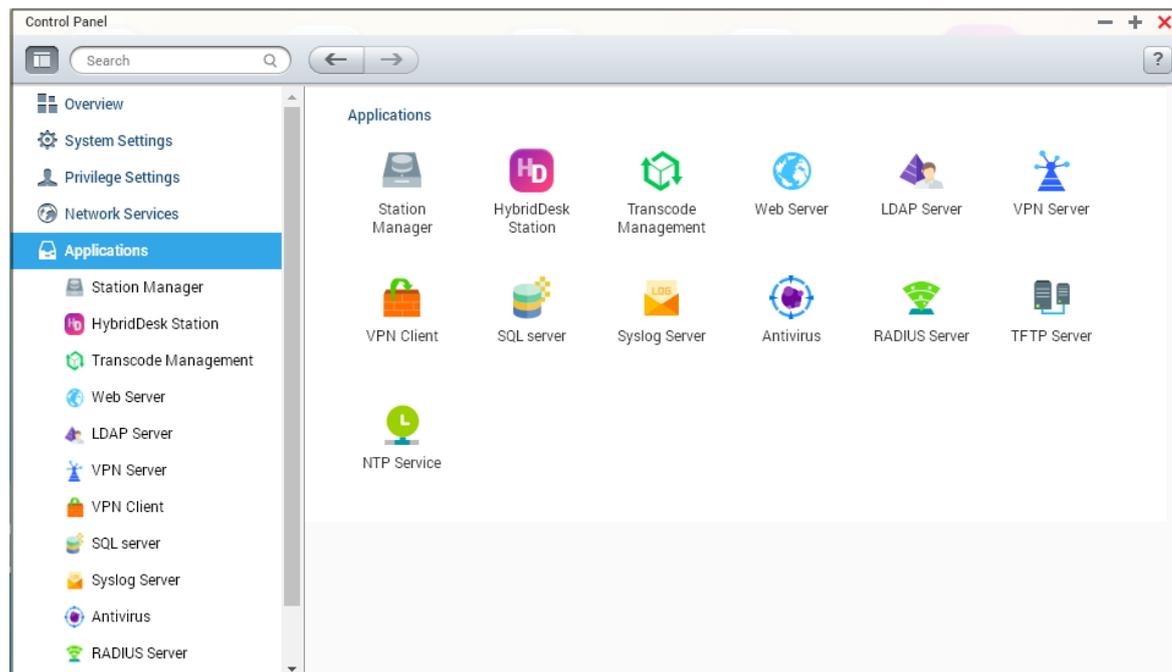
1. Log into the QGW series as an administrator and navigate to the "Devices" page in Qsync Central Station.
2. Click the "Edit settings for Qsync utility" icon under "Action" for the device to be modified
3. Modify its preference settings (including synchronization, policy and mail settings.)

To set a management password, follow these steps:

1. Log into the QGW series as an administrator and navigate to the "Management Settings" page in Qsync Central Station.
2. Select Central Configuration Mode.
3. Tick "Enable your management password".
4. Enter the password and click "Lock".

# Business Applications

The following QGW series functions are designed to meet business needs.



For setup details, refer to the following links:

- [Antivirus](#)
- [Backup Station](#)
- [File Station](#)
- [LDAP Server](#)
- [SQL Server](#)
- [NTP Service](#)
- [RADIUS Server](#)
- [Syslog Server](#)
- [TFTP Server](#)
- [Virtualization](#)
- [VPN Client](#)
- [VPN Server](#)
- [Web Server](#)

# Antivirus

Configure antivirus features on this page.

Overview Scan Jobs Reports Quarantine

Antivirus

Enable antivirus

Virus definitions: 2015/12/16 00:36

Last virus scan: --

Last infected file found: --

Status: Update complete

Update

Check and update automatically. Frequency in days:

Online update:

Manual update (\*.cvd):

## Overview

- **Antivirus:** Use the antivirus to scan the QGW series manually or on recurring schedules. It will delete, quarantine, or report files infected by viruses, malware, Trojans, and other malicious threats. To use this feature, select "Enable antivirus" and click "Apply".
- **Update:** Select "Check and update automatically" and specify the intervals in days to automatically update the antivirus definitions. Click "Update Now" to check for new antivirus definitions and to update if necessary. Users can also download updated definitions from <http://www.clamav.net> and manually update the antivirus definitions. The QGW series must be connected to the Internet to use this feature.
- **Quarantine:** View the quarantine information of the disk volumes on the QGW series. For more details, go to "Applications" > "Antivirus" > "Quarantine".

**Note:** The antivirus engine selector next to the "Enable antivirus" checkbox is only available after an antivirus App has been installed from the [App Center](#).

## Scan Jobs

The QGW series supports manual and scheduled scanning of all or specific shared folders. Up to 64 schedules can be created and up to 5 scan jobs can run concurrently. To create a scan job, follow these steps.

1. Go to "Applications" > "Antivirus" > "Scan Jobs". Click "Add a Scan Job".
2. Enter the job name and select the shared folders to scan. To scan a specific shared folder, select the share folder and click "Add".
3. Multiple shared folders can be selected. To remove a shared folder, click the "Delete (X)" button next to the share name and click "Next". Define the scan job schedule and click "Next".
4. Select to scan all the files in the shared folder(s) or quick scan to scan only potentially dangerous files. Select "Exclude files or folders" and specify a file, a folder, or a file extension to be excluded from the virus scan and click "Next". Separate each entry with a space in the same line or enter one entry per line. For example:
  - /Public/testfile.txt
  - /Download
  - \*.log
  - \*.exe \*.com
  - \*.txt; click "Next".
5. Enable other scan options and click "Next":
  - Specify the maximum file size (1-4096 MB) allowed for scanning.
  - Enable "Scan compressed files" to include these files in shared folders. Specify the maximum amount of data (1-4096 MB) in a compressed file for scanning (if applicable). The maximum compressed file size may vary based on the QGW model and available memory.
  - To scan MS Office and Mac Office files, RTF, PDF, and HTML files, select "Deep scan for document files".
6. Specify the actions to take when infected files are discovered and click "Finish" to create the scan job.
  - Only report the virus: The virus scan reports are recorded under the "Reports" tab. No actions will be taken for the infected files.
  - Move infected files to quarantine: The infected files will be quarantined and cannot be accessed from their original shared folders. Users can view the virus scan reports under the "Reports" tab and delete/restore the infected files under the "Quarantine" tab.
  - Delete infected files automatically: Infected files will be deleted and cannot be recovered.
  - To receive an alert email when an infected file is found or after scanning has completed, configure the SMTP server settings in "System Settings" > "Notification" > "SMTP Server".
7. The scan job will run according to its schedule.

Button	Name	Description
	Run	Run the scan job now.

	Stop	Stop the scan job.
	Edit	Edit the scan job settings.
	View last run log	Open the last virus scan summary.
	Delete	Delete the scan job.

## Reports

View or download the reports of the latest scan jobs on the QGW series.

Button	Name	Description
	Download	Download the virus scan report. The file can be opened by any text editor.
	Delete	Delete an entry on the list.
DOWNLOAD	Download All	Download all the virus scan logs on the list as a zip file.

## Report options

- Specify the number of days (1-999) to retain the logs
- Enable the option "Archive logs after expiration" and specify the shared folder to save the logs to once the retention period has been reached. Click "Apply All" to save the changes.

## Quarantine

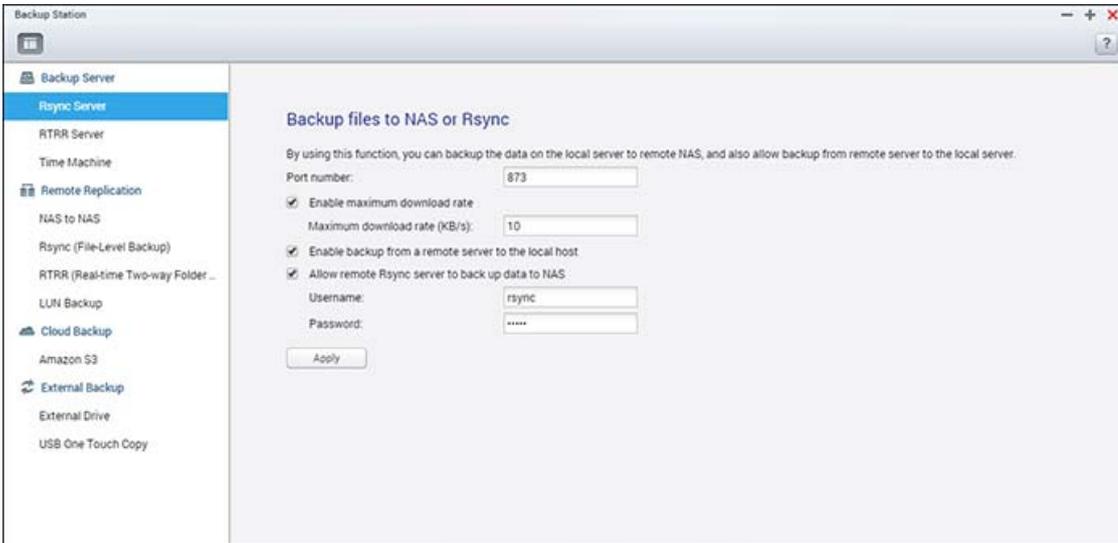
This page shows the quarantined files on the QGW series. Users can manually delete or restore quarantined files, or restore and add the files to the exclude list.

Button	Name	Description
	Delete	Delete an infected file. The file cannot be recovered.
	Restore	Restore an infected file to its original shared folder.
	Exclude List	Restore an infected file and add the file into the exclude list (scan filter).
Restore Selected	Restore Selected Files	Restore multiple files on the list.

Files		
Delete Selected Files	Delete Selected Files	Delete multiple files on the list. The files cannot be recovered.
Delete All Files	Delete All Files	Delete all of the files on the list. The files cannot be recovered.

# Backup Station

Configure the QGW series as a backup server, remote replication, cloud backup and external backup with the Backup Station.



For details on the features, please refer to the following links:

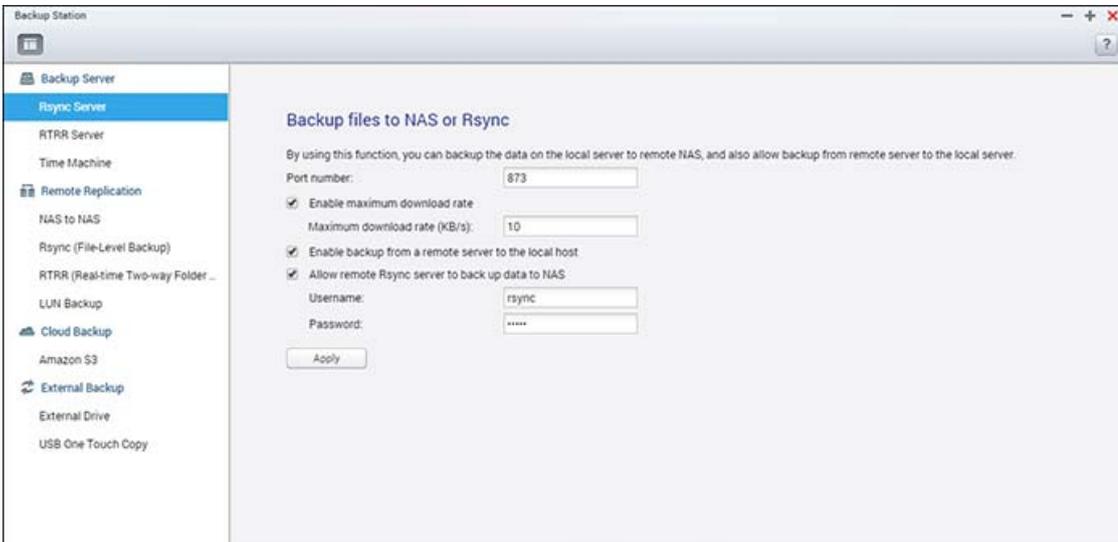
- [Backup Server](#)
- [Remote Replication](#)
- [Snapshot Replica](#)
- [Cloud Backup](#)
- [External Backup](#)

**Note:** Snapshots and related features are currently only available for the following QGW series.

- A minimum of 4 GB RAM is required to use snapshots.
- Support up to 256 snapshots instead of 1024.

# Backup Server

## Rsync Server

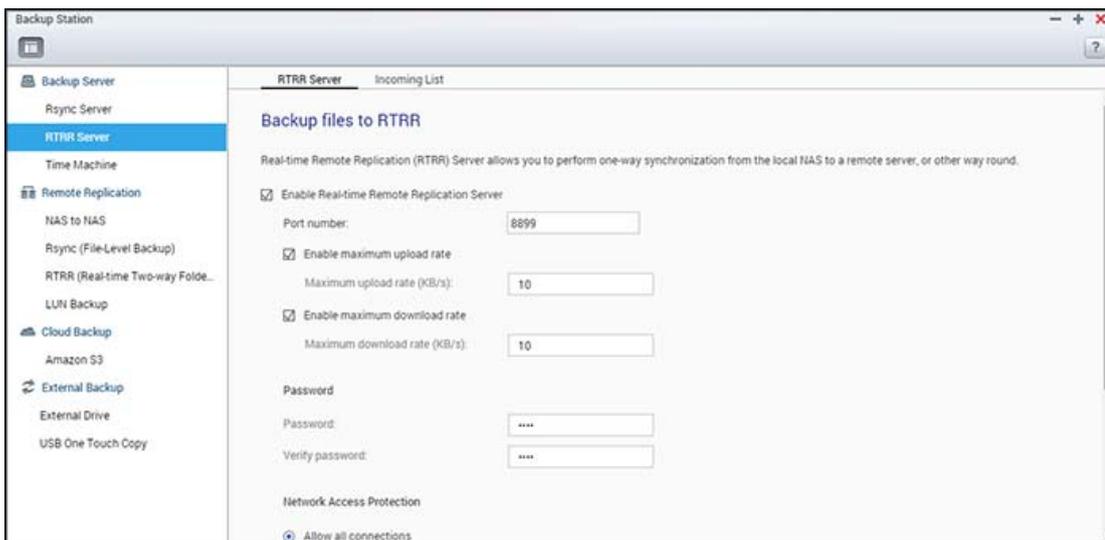


Enable Rsync server to configure the QGW series as a backup server for data backup from a remote Rsync server or NAS server. The default port number for remote replication via Rsync is 873. Specify the maximum download rate for bandwidth control. 0 means unlimited.

- **Enable backup from a remote server to the local host:** Select this option to allow data backup from a remote server to the local server.
- **Allow remote Rsync server to back up data to the QGW series:** Select this option to allow data backup from an Rsync server to the local server. Enter the username and password to authenticate the Rsync server which attempts to back up data to the QGW series.

**Note:** You can only create up to 64 rsync jobs on the QGW series.

## RTRR Server



To allow real-time or schedule data replication from a remote server to a local QGW system, select "Enable Real-time Remote Replication Server". You can specify the port number for remote replication. The default port number is 8899. Specify the maximum upload and download rate for bandwidth control. 0 means unlimited. To only allow authenticated access to back up data to the local QGW system, specify the access password. The client server will be prompted to enter the password to back up data to the QGW system via RTRR.

You can specify the IP addresses or host names which are allowed to access the QGW system for remote replication. Up to 10 rules can be configured. To allow all connections, select "Allow all connections". To specify IP addresses or host names, select "Allow connections from the list only" and click "Add".

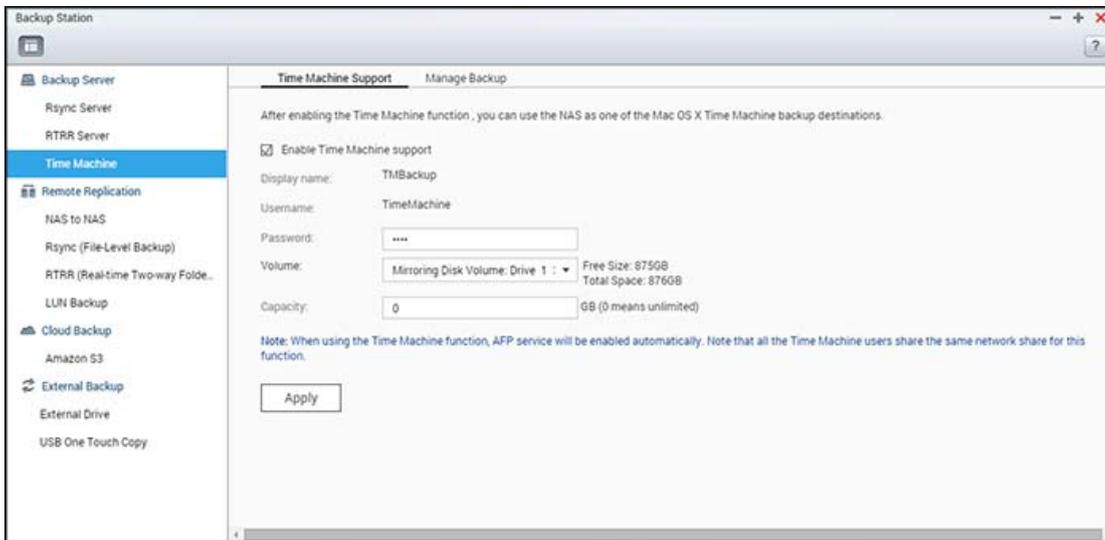
Enter an IP address or specify a range of IP addresses by entering the IP and subnet mask. Select the access right "Read Only" or "Read/Write". By selecting "Read/Write", the client server is allowed to delete files on the local QGW system. Click "Finish" to exit. After saving the access rule, click "Apply" and the QGW system will restart to apply the settings.

### Check backup jobs from other QGW system

You can check and manage backup jobs from other QGW system that use the current QGW system as a target destination for their backup. To check backup jobs, click the "Incoming List" tab and the details (including the job name, source system, destination system, job schedule and job status) of the backup jobs will be shown in the list. You can also manage backup jobs in this list. To do so, select backup jobs under "Incoming List" > choose to clear job records, open the backup folder, or deny access of the backup jobs to your QGW system.

## Time Machine

You can enable Time Machine support to use the QGW series as a backup destination for Macs by the Time Machine feature on OS X.



To use this function, follow these steps.

Configure the settings on the QGW series:

1. Enable Time Machine support.
2. Enter the Time Machine password. The password is empty by default.
3. Select a volume on the QGW series as the backup destination.
4. Enter the storage capacity that Time Machine backup is allowed to use. The maximum value is 4095GB, 0 means unlimited.
5. Click "Apply" to save the settings.

All the Time Machine users share the same shared folder for this function. Configure the backup settings on Mac:

1. Open Time Machine on your Mac and click "Select Backup Disk".
2. Select the TMBBackup on your QGW series from the list and click "Use for Backup".
3. Enter the username and password to login to the QGW series and click "Connect".
  - o Registered username: TimeMachine
  - o Password: The password you have configured on the QGW series. It is empty by default.
4. Upon successful connection, the Time Machine is switched "ON". The available space for backup is shown and the backup will start in 120 seconds.

The first backup may take more time according to the data size on the Mac. To recover data to the Mac OS, please see a tutorial on <http://www.apple.com>.

## Managing Backup

You can manage existing backups on this page.

- Volume (drop down menu on top right side of the screen): Display Time Machine backup tasks stored in the volume.
- Name: The name of the Time Machine backup (the sparse bundle disk image which was created by Time Machine.)
- Size: Size of this Time Machine backup.
- Date Modified: Last modified date of this Time Machine backup.
- Delete: Delete the selected Time Machine backup.

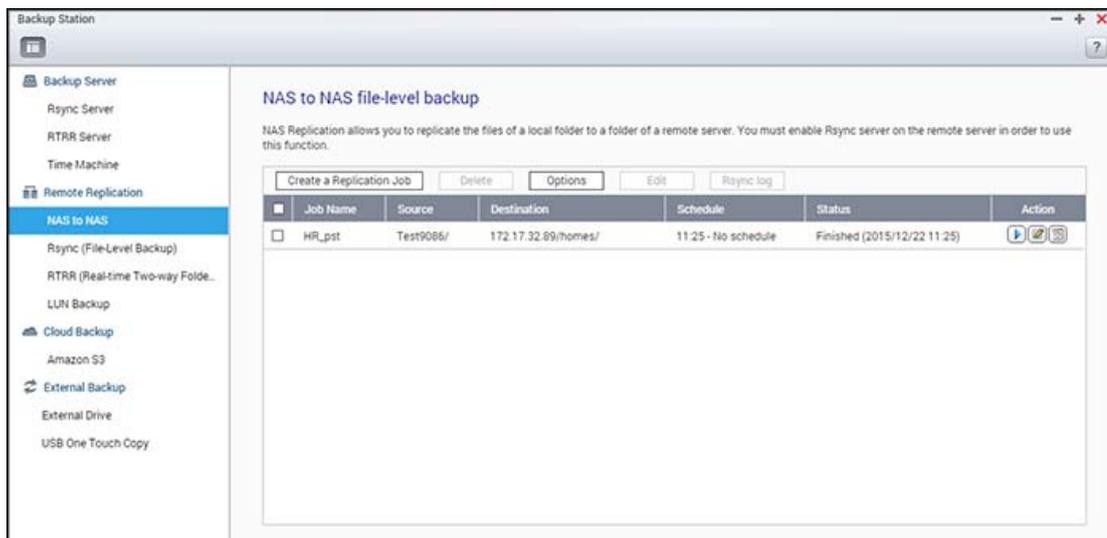
# Remote Replication

This chapter covers the following topics:

- [NAS to NAS and Rsync](#)
- [RTRR](#)
- [Downloading Replication Job Logs](#)

## NAS to NAS and Rsync

The QGW series data can be backed up to a remote NAS or Rsync server using Rsync remote replication.



If the backup destination is a NAS, go to "Main Menu" > "Backup Station" > "Rsync Server" and enable the remote NAS as an Rsync backup server.

1. To create a replication job, click "Create a Replication Job".
2. Specify the server type (NAS or Rsync server) of the remote server. Enter a job name. Click "Next".
3. Enter the IP address, port number, username and password to login to the remote server. The default port number is 873. The login username must have read/write access to the remote server and a sufficient quota limit on the server. Click "Test" to verify the connection, then click "Apply".
4. Specify the local folder by clicking the Source folder box. After expanding and locating the folder, double click on it to set it as the directory where the data will be replicated from.
5. Specify the destination folder Destination folder box. Locate the folder in the folder tree and double click on it to set it as the directory where the data will be replicated to. And, click "Add" to add this pair of replication folders.
6. Click "Backup frequency" to configure the backup frequency. Select to immediately replicate the data or to specify a backup schedule.

7. Specify the following options for remote replication jobs by clicking "Options" and click "Apply".
  - Enable encryption: Select this option to execute encrypted remote replication. Note that you must enable "Allow SSH connection" in "Network Services > "Telnet/SSH" and specify the same port number for SSH and encrypted remote replication.
  - Activate file compression: Allows file compression during the data transfer process. This option is recommended for low bandwidth environments or remote replication over WAN.
  - Perform incremental replication: When this option is enabled, after the first-time replication, the QGW series will only back up files that have been changed since the last backup. The files of the same name, size, and modified time will not be copied again. Enabling this option is recommended for replication jobs that will be executed multiple times in order to shorten the backup time.
  - Delete extra files on remote destination: Select this option to synchronize the source data with the destination data (one-way synchronization.) Extra files on the destination will be deleted. Source data will remain unchanged.
  - Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turning on this option may reduce the time required for remote replication.
8. Click "Apply". If you selected "Execute backup immediately", the replication task will start at once. Otherwise it will be performed according to your schedule. Note that the job is recursive. Do not turn off the local QGW system and the remote server when remote replication is running.

**Note:** For step 5, the order of selecting the source and destination folders can be changed. The above is just an example.

Icon	Name	Description
	Start	Start a replication job immediately.
	Stop	Stop a running replication job.
	View	View Rsync logs (replication results).
	Edit	Edit a replication job.
	Disable	Disable replication schedule.
	Enable	Enable replication schedule.

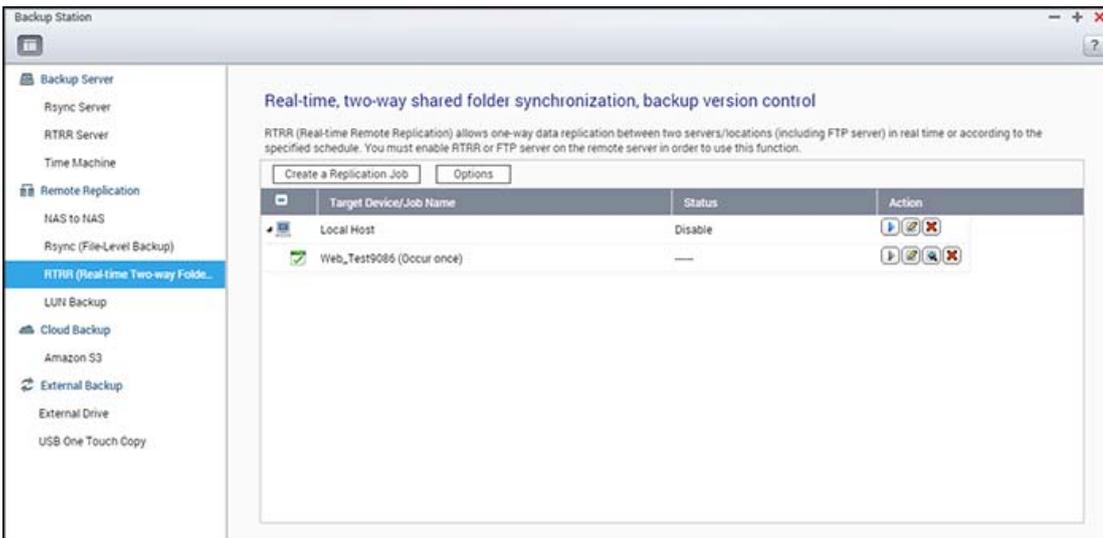
To configure the timeout and retry settings of the replications jobs, click "Options".

- Timeout (second): Specify a timeout value for each replication job. This is the maximum number of seconds to wait until a replication job is cancelled if no data has been received.

- Number of retries: Specify the number of times the QGW series should try to execute a replication job if it fails.
- Retry intervals (second): Specify the number of seconds to wait in between each retry.

For example, if you entered 600 seconds for timeout, 3 retries, and 60 seconds for retry intervals, a replication job will timeout in 600 seconds if no data is received. The QGW series will wait for 60 seconds and try to execute the job a second time. If the job timed out again, the QGW series wait for another 60 seconds and retry for a third and final time.

## RTRR



Real-time Remote Replication (RTRR) provides real-time or scheduled data replication and one-way and two-way data synchronization between two locations (such as a local NAS and a remote NAS, local NAS and an FTP server, or local NAS and an external drive, or replication between two local folders.) In real-time mode, the source folder will be monitored and any files that are new, changed, and renamed will be immediately replicated to the target folder. In scheduled mode, the source folder will be replicated to the target folder according to the pre-defined schedule.

One way synchronization refers to data synchronization from the source to the destination, while two-way synchronization means both the source and destination are synchronized after new files are copied in either side or files stored on either side are changed or deleted.

If the backup destination is a NAS, the RTRR server ("Main Menu" > "Backup Station" > "RTRR Server") or FTP service must first be enabled ("Main Menu" > "Control Panel" > "Network Services" > "FTP") on the remote NAS.

\*Each job supports up to 16 folder pairs.

Follow these steps to create a replication job.

1. Click "Create a Replication Job".

2. When the wizard shows up, click "Next".
3. Select the synchronization locations and click "Next". Make sure the destination device has been formatted and folders have been created. Select the action to take (Backup, Synchronize, or Restore), the synchronization locations, and click "Next". Make sure the destination device has been formatted and folders have been created. For comparison between available actions and their folder pairs, refer to the following table:

<b>Action</b>	<b>Direction</b>	<b>Local folder to remote folder</b>	<b>Local folder to local folder/external drive</b>	<b>Remote folder to local folder</b>
Backup		✓	✓	
Synchronization		✓	✓	✓
Restoration			✓	✓

Two synchronization options are available: one-way synchronization and two-way synchronization.

- For one-way synchronization, you can choose to:
    - Synchronize data from a local folder to a remote folder (NAS or FTP server)
    - Synchronize data from a remote folder (NAS or FTP server) to a local folder
    - Synchronize data from a local folder to another local folder or an external drive
  - For two-way synchronization, you can choose to:
    - Synchronize data between the source and destination
4. Enter the IP address or host name. Select the server type (Windows Share (CIFS/SMB), FTP server or NAS server with RTRR service enabled; For two-way synchronization, only the NAS server is available.)
    - **Remote replication to FTP server:** Specify the port number and if you want to enable FTP with SSL/TLS (Explicit) for encrypted data transfer. If the FTP server is behind a firewall, enable passive mode. Enter the username and password with read/write access to the server. Click "Next".
    - **Remote replication to NAS with RTRR service:** Enter the IP address of the RTRR service-enabled server. Specify the connection port and select whether or not to enable secure connection. The default port number for remote replication via RTRR is 8899. Enter the password for RTRR connection. Click "Next".
    - **Remote replication to Windows Share (CIFS/SMB):** Enter the IP address of the Windows server. Specify the destination folder, username and password and click "Next".
  5. Select the folder pair for data synchronization.
  6. Each sync job supports up to 5 folder pairs. Select more folder pairs and click "Add". Click "Next".

7. Choose between real-time and scheduled synchronization. Real-time synchronization copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup. Scheduled synchronization copies files from the source folder to the target folder according to the pre-configured schedule. The options are:
- Replicate Now: Replicate data immediately.
  - Periodically: Enter the time interval in hours and minutes that the backup should be executed. The minimum time interval is 5 minutes.
  - Hourly: Specify the minute when an hourly backup should be executed (for example, enter "01" to execute backup on the first minute of every hour.)
  - Daily: Specify the time when a daily backup should be executed (for example: 02:02 every day.)
  - Weekly: Select a day of the week and the time when a weekly backup should be executed.
  - Monthly: Select a day of the month and the time when a monthly backup should be executed.
  - Occurs once at: Specify the date and time the scheduled replication job will once be executed and this replication job will be executed only once.

**Note:**

- If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a replication job, you cannot select the folder as the source or destination of another folder pair of the same job.
- You can also create a folder as you select the folder pair. To do so, enter the folder name and click the folder icon from the drop down list.
- Two-way synchronization only supports scheduled data replication.
- The expiration time setting is not available for "Replicate Now" and "Occurs once at" in Step 7.

8. To configure synchronization policy, select "Configure policy and filter" and click "Next". Select whether or not to enable the following options:
- Delete extra files: Delete extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time synchronization.
  - Detect sparse files: Select this option to ignore files of null data.
  - Check file contents: Specify to examine file contents, date, size, and name to determine if two files are identical. This option is not available for real-time synchronization.
  - Compress files during transmissions: Specify whether or not the files should be compressed for synchronization operations. Note that more CPU resources will be used.
  - Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.
  - Extended attributes: Select this option to keep the information in extended attributes.
  - Timeout and retry settings: Specify the timeout period and retry settings if a synchronization operation fails.

9. Specify the file size, file types to include/exclude, and file date/time to filter data synchronization.  
Enter a job name.
  - File size: Specify the minimum and maximum size of the files to be replicated.
  - Last modified: Specify the number of days files are last modified for replication.
  - Include file types: Specify the file types to be replicated.
  - Exclude file types: Specify the file types to be excluded for replication.
  - File date/time: Specify the date and time of the files to be replicated.
10. Click "Next".
11. Confirm the settings and click "Next".
12. Click "Finish" to exit the wizard.

Icon	Name	Description
	Enable and Start	Enable connection to a remote server. Start a replication job.
	Stop	Stop connection to a remote server or external drive.
	Stop	Stop a replication job.
	View	View job status and logs; download logs.
	Edit	Edit the connection settings of a remote server. Edit the settings of a replication job.
	Delete	Delete connection settings to a remote server. Delete a replication job. This button is available only after a replication job is stopped or the connection to the remote server is stopped.

To edit the replication job properties, click "Options".

Under "Event Logs" you can enable "Download Detailed Logs" and specify the maximum file size of log files. You can also set up sending email alerts when synchronization fails or completes. SMTP server settings must be set up on the QGW series before using email alerts ("System Settings" > "Notification".)

Specify the replication policy in "Policy" and filter settings in "Filter". These will become the default settings for all RTRR replication jobs.

## **Downloading Replication Job Logs**

To view the status and logs of a replication job, click the "View" button under "Action". You can view job logs or download them by clicking "Download Logs". Log files can be opened by Microsoft Excel or text editors. This button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed at least one replication job.

# Snapshot Replica

The Snapshot Replica allows you to replicate the volume/LUNs between different remote servers using snapshot technology, which provides a flexible and efficient backup service for IT professionals.

To use this function, please enable the SSH server ("Control Panel" > "Network Services" > "Telnet/SSH") on the remote QGW system first. Note that you may also access this function via Storage Manager ("Storage Manager" > "Storage Space"> "Snapshot" > "Snapshot Replica" for volumes or "Storage Manager" > "iSCSI Storage"> "Snapshot" > "Snapshot Replica" for LUNs.)

**Note:** Snapshots and related features are currently only available for the following models.

- \* A minimum of 4 GB RAM is required to use snapshots.
- \* Support up to 256 snapshots instead of 1024.

## Creating Replication Jobs

Follow these steps to create a snapshot replication job.

1. Click "Create a Replication Job".
2. Enter a name for this job.
3. Click "Settings" to specify the settings for the remote server. Enter the IP address, username and password for the remote server. Check "Local site" if the replication job is for your local QGW series. Note that the login account must have read/write access to the remote server and sufficient quota limit on the server. Click "Test" to verify the connection. Then click "OK".
4. Select the local volume to take snapshot of by clicking the "Source Volume/LUN" drop-down list.
5. Select the destination pool to store the snapshots in the "Destination Pools" box.
6. Keep Snapshots: The maximum number is 1024. The system keeps this fixed number of versions and automatically rotates stored versions.
7. Click "Backup frequency" to configure the backup frequency. Select to replicate the data immediately or specify the backup schedule.
8. Specify other options as follows for the remote replication job by clicking the "Options" button and click "OK" after setup.
  - o Enable encryption: Select this option to execute encrypted remote replication. Note that you must enable "Allow SSH connection" in "Network Services > "Telnet/SSH" and specify the same port number for SSH and encrypted remote replication.
  - o Enable maximum transfer rate: Enter the value to restrict maximum available bandwidth in KB/s. If it is not specified, the bandwidth for this job is not limited.
  - o Compress files during transmission: Enable this option to allow file compression during the data transfer process. This option is recommended for a low bandwidth environments or remote replication over WAN.

9. Click "OK". If you select the "Execute backup immediately" option, the replication task will start at once. Otherwise, it will be performed according to your schedule. Note that the job is recursive. Do not turn off the local QGW series and the remote server when remote replication is running.

Icon	Name	Description
	Enable and Start	Enable connection to a remote server. Start a replication job.
	Stop	Stop a replication job.
	View	View job status and logs; clear logs.
	Edit	Edit the settings of a replication job.
	Enable/Disable Schedule	Enable or disable a scheduled replication job.

The system displays logs of all replications jobs at the bottom of the screen. Click "Clear all logs" to clear job logs.

### Deleting Replication Jobs

1. Select a replication job from the list.
2. Click "Delete".
3. Click "OK".

### Options

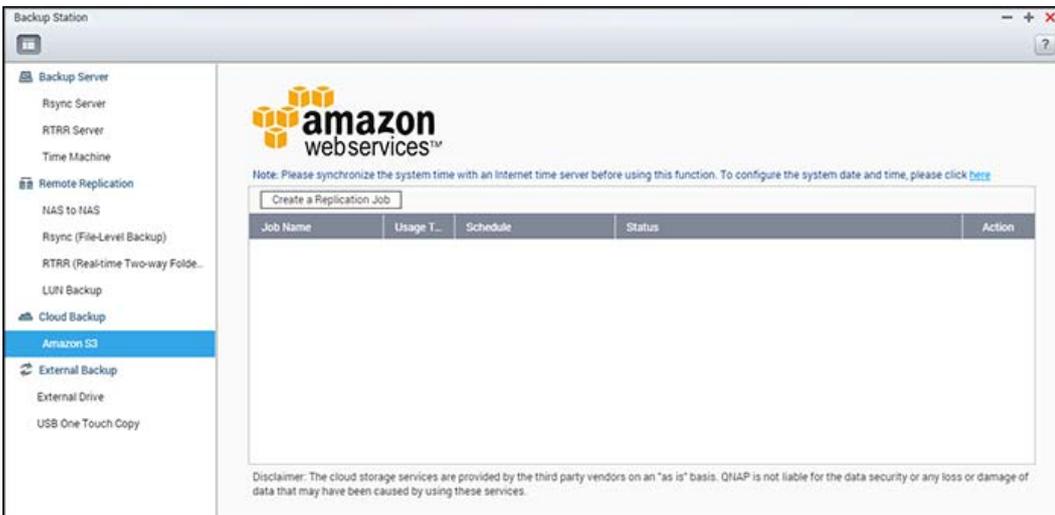
To change connection options, click "Options" and specify the timeout period of the number of connection retries.

In case the password used for access to the remote server is changed, you can click "Change Password" and click the "edit" button under "Action" to change the password used for that server.

# Cloud Backup

## Amazon S3

Amazon S3 (Simple Storage Service) is an online storage web service offered by AWS (Amazon Web Services.) It provides a simple web service interface that can be used to store and retrieve data from anywhere on the web. With Amazon S3, you can upload data from your QGW series to Amazon S3 or download the data from Amazon S3 to your QGW series. You need to register an AWS account from <http://aws.amazon.com> and pay for the service. After signing up, you need to create at least one bucket (root folder) on Amazon S3 using an Amazon S3 application. We recommend the Mozilla Firefox add-on "S3Fox" for beginners.



After setting up the Amazon S3 account, follow these steps to back up or retrieve data from Amazon S3 using the QGW series.

1. Click "Create a Replication Job".
2. Enter the remote replication job name.
3. Select the usage type: "Upload" or "Download" and enter other settings. A bucket is the root directory on Amazon S3. You can test the connection to the remote host testing by clicking "Test". Other settings are optional.
4. Specify the local directory on the QGW series for replication.
5. Enter the replication schedule.
6. Click "Finish". The replication job will be executed according to your schedule.

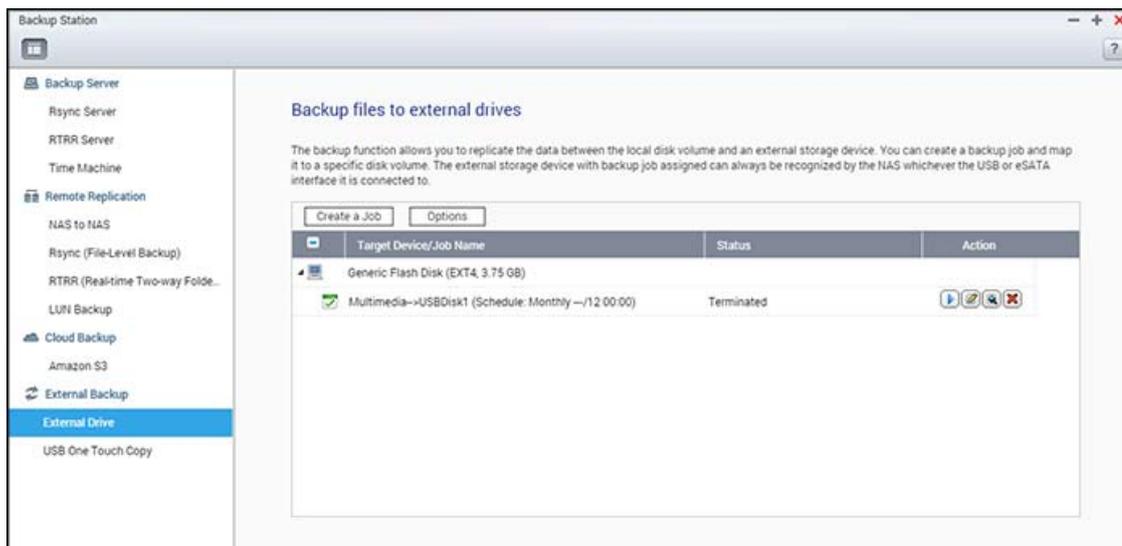
# External Backup

The following topics are covered in this chapter:

- [External Drive](#)
- [USB One Touch Copy](#)

## External Drive

The QGW series supports real-time and scheduled data backup between internal disks volumes on the QGW series and external USB storage devices.



To use this feature, follow these steps.

**Note:** If an external storage device is encrypted by the QGW series, make sure it is unlocked in "External Device" > "External Storage" before creating any backup jobs.

1. Connect one or more storage devices to the USB interfaces of the QGW series.
2. Click "Create a new job".
3. When the wizard is shown, read the instructions carefully and click "Next".
4. Select the backup locations.
  - a. Select an external disk volume from the drop-down menu. The QGW series supports EXT3, EXT4, FAT, NTFS, and HFS+. The storage device's general information will be shown.
  - b. Select "Map this backup job to the volume ID only" to map the backup job to this particular external storage device. The QGW series will recognize the device and automatically execute the backup job according to the settings every time it is connected to the QGW series via any USB interface.

- c. Select to back up the data from a local disk volume to the external storage or vice versa.
  - d. Click "Next".
5. Select the source and destination folders for backup. Then click "Add". Up to 128 folder pairs can be created. Click "Next".

**Note:**

- Multiple partitions on the external storage device will be recognized as individual disk volumes.
- If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a backup job, the same folder cannot be selected as the source or destination of another folder pair of the same backup job.
- External Drive supports up to 16 jobs and each job supports up to 8 folder pairs.

6. Choose between real-time and scheduled backup. Real-time backup copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup. Scheduled backup copies files from the source folder to the target folder according to the schedule. The options are:
- Replicate Now: Copy the data immediately.
  - Periodically: Enter the time interval in hours and minutes that the backup job should be executed. The minimum time interval is 5 minutes.
  - Hourly: Specify the minute when an hourly backup should be executed (for example, enter "01" to execute backup on the first minute of every hour).
  - Daily: Specify the time when a daily backup should be executed (for example: 02:02 every day).
  - Weekly: Select a day of the week and the time when a weekly backup should be executed.
  - Monthly: Select a day of the month and the time when a monthly backup should be executed.
  - Auto-Backup: Execute data backup automatically every time the device is connected and detected by the QGW series.
7. Choose to automatically eject the external drive after the job is finished.
8. To configure the backup policy and filter settings, select "Configure policy and filter" and click "Next". Select whether or not to enable the following options:
- Delete extra files: Deletes extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time data backup.
  - Detect sparse files: Select this option to ignore files with null data.
  - Overwrite the file if the source file is newer or the file size is different .

- Check file contents: Examine the file contents, date, size, and name to determine if two files are identical. This option is not available for real-time data backup.
  - Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.
9. Create filters for the backup job.
    - File size: Specify the minimum and maximum sizes of the files to be copied.
    - File date/time: Specify the date and time of the files to be copied.
    - Include file types: Specify the file types to be copied.
    - Exclude file types: Specify the file types to be excluded from the data copy.
  10. Enter a name for the backup job. A job name supports up to 63 characters and cannot start or end with a space.
  11. Confirm the settings and click "Next".
  12. Click "Finish" to exit the wizard.
  13. The backup job and the status will be shown on the list.

Button	Name	Description
	Start	Start a backup job.
	Stop	Stop a backup job.
	Edit	Edit the backup job.
	View / Download	View the job status and logs. Download the backup job logs.
	Delete	Delete a backup job. This button is only available after a backup job is stopped.

To disable a backup job's schedule, click "Edit" and select "Disabled" under "Settings" > "Schedule Type" and click "OK".

### Default Backup Job Settings

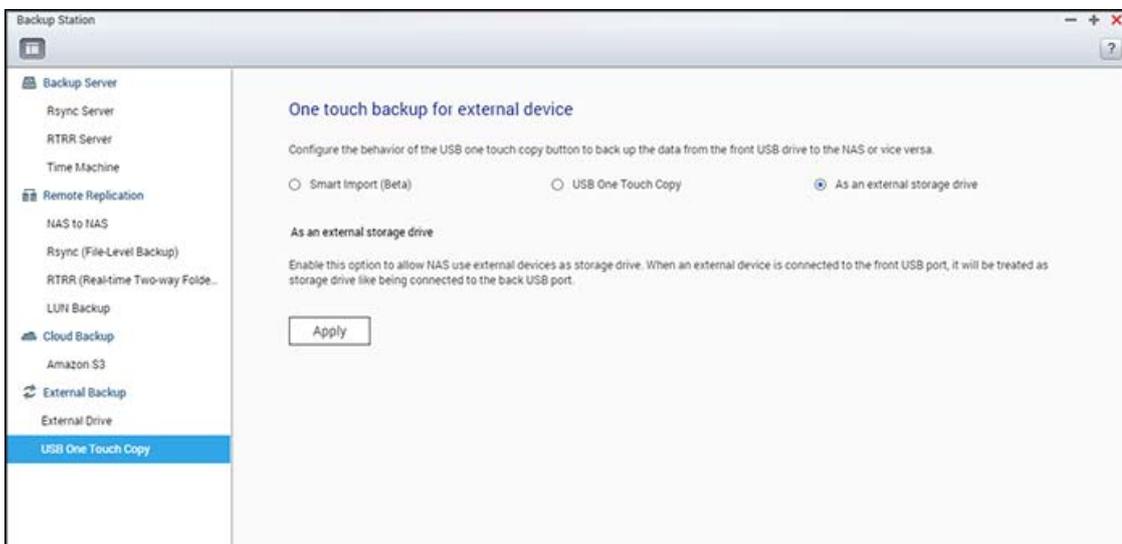
1. To edit the default backup job properties, click "Options".
2. Under "Event Logs" you can select to enable "Download Detailed Logs" and specify the maximum file size of the log file. Select to send an email alert when a backup job fails or completes. Note that the SMTP server settings must be properly set up in "System Settings" > "Notification".
3. Specify the backup policy in "Policy" and filter settings in "Filter". These will become the default settings for all the backup jobs.

## Download Backup Logs

1. To download a backup job's logs, make sure the option "Download Detailed Logs" is enabled in "Options" > "Event Logs".
2. Click the "View / Download" button in "Action" column of a backup job.
3. Go to "Job Logs" and click "Download Logs". The log file can be opened by Microsoft Excel or any text editor. This button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed a backup job.

## USB One Touch Copy

Enable the USB one touch copy button to back up data from USB storage connected to the front-panel USB port to the QGW series or vice versa.



## Smart Import (Beta)

When a USB device (such as a camera) is connected to the front USB port, all of the photos and videos on the device will be automatically imported to the QGW seriesS without pressing the "Copy" button. Imported files will be stored in "SmartImport," a newly-created folder, under the default backup directory. During each import, only new photos and videos will be imported to a new folder.

## USB One Touch Copy

For customized backup configuration, please select "USB One Touch Copy."

- Backup direction: From the front USB drive to the QGW series or vice versa.
- Backup method:
  - Create directory: A new directory will be created on the destination and the source data will be copied to this directory. The new directory will be named as the backup date (YYYYMMDD). If there are two or more backups on the same day, the directory will be named with YYYYMMDD-1, YYYYMMDD-2... and so on.

- Copy: Back up data to the destination share. If the same file exists, the destination file will be overwritten.
- Synchronize: Back up data to the destination share and clear the redundant files. If the same file exists, the destination file will be overwritten.
- Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turn on this option may reduce the time required for backup.
- Source and destination folders: Specify the folder pairs for backup and click "Add". Maximum 9 folder pairs can be added.
- Options: Click "Options" to set up notification of the backup jobs by email, SMS, or instant messaging (IM).
- Unmount the front USB drive manually: When enabled, users can press the Copy button for about 8–10 seconds until the USB LED light turns off and remove the front USB drive from the QGW series.
- Enable the alarm buzzer:
  - One short beep: Backup has started.
  - Two short beeps: The front USB drive is being unmounted.

**Note:** If there are multiple partitions on the source storage device, a new folder will be created for each partition on the destination as the backup folder. The backup folder will be named with the backup date and the partition number (YYYYMMDD-1 for partition 1, YYYYMMDD-2 for partition 2, etc). If the source storage device only contains one partition, the backup folder will be named YYYYMMDD.

### Data copy using front USB port

The QGW series supports instant data copy backup from USB devices to the QGW series or vice versa using the one touch copy button. To use this function, follow these steps:

1. Make sure a hard drive is installed and formatted on the QGW series.
2. Configure the behavior of the Copy button in "Backup Station" > "USB One Touch Copy".
3. Connect the USB device to the front USB port of the QGW series.
4. Press the Copy button once. The data will be copied according to your settings.

**Note:** Incremental backup is used for this feature. After the first data backup, the QGW series only copies the files changed since the last backup.

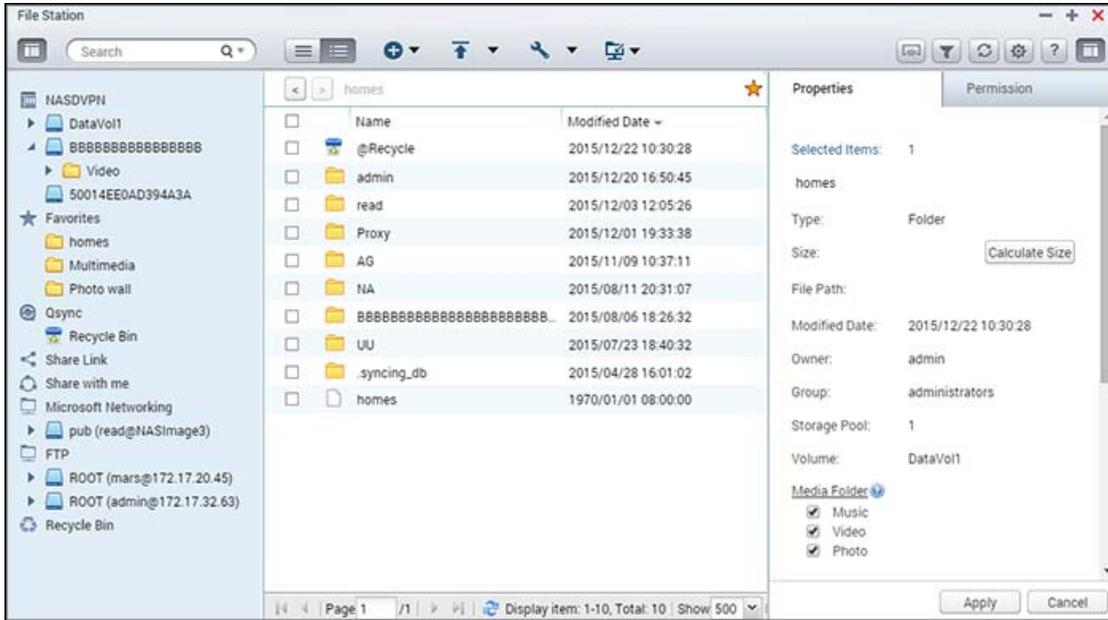
**Caution:** Files are copied from the source to the destination. **Extra files in the destination will be deleted. Files with the same names will be overwritten by the source.** Source data will remain unchanged.

**As an external storage drive**

When an external device is connected to the front USB port, it will be identified as an external storage drive connected to the port.

# File Station

File Station is an online file management center. With the File Station, you can access the QGW series across the Internet, manage files using a web browser, quickly find files, play media files, set file and folder permissions, and easily share your files and folders on the QGW series.



Topics covered in this chapter:

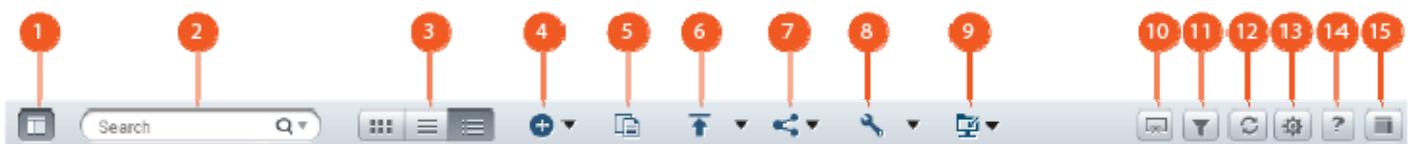
- [Starting File Station](#)
- [Familiarizing yourself with File Station](#)
- [Using File Station](#)
- [Remote Connection](#)

## Starting File Station

Launch File Station from the Main Menu/Desktop shortcut, or directly log into File Station by going to: [http://QGW\\_Name\\_or\\_IP/cgi-bin/filemanager.html](http://QGW_Name_or_IP/cgi-bin/filemanager.html).

## Familiarizing yourself with File Station

### Menu Bar



No.	Name	Description
1	Left Panel	Hide/Show the left panel.
2	Search Bar	Search files by their name, file type (video or photo) or with advanced search.
3	Browsing Mode	Switch between different browsing modes (from left to right: Thumbnail browsing mode/list browsing mode/detail browsing mode.)
4	Create	Create a folder/shared folder or share space with a user (see the below <a href="#">Sharing space</a> section.)
5	Copy/Paste	Copy/paste folders or/and files.
6	Upload	Upload files or folders to the selected shared folder.
7	Share	Share the folder/file via email, publish the folder/file, or share the link of the folder/file on social networks and to existing QGW users, or create a shared link (see the below <a href="#">Sharing files</a> section.)
8	More Action	<ul style="list-style-type: none"> <li>• Bookmark the selected shared folder (and it will appear under "Favorites" on the left panel.)</li> <li>• Perform file or folder operations including open, download, rename, copy/move, delete, cut, create desktop shortcut, compress, transcode files/folders (these options are only available when files and/or folders are selected.)</li> <li>• Check folder properties.</li> <li>• Review transcode information, background tasks (file compression, file upload and moving files within the QGW series) or storage information.</li> </ul>
9	Remote Connection	<ul style="list-style-type: none"> <li>• Create remote connections</li> <li>• Check connection records and the current connection status (see the below <a href="#">Remote Connection</a> section.)</li> </ul>
10	Network Media Player	Stream videos to compatible devices in different rooms over your home network.
11	Smart File Filter	Filter files based on conditions set by users and the conditions will apply to all folders.

12	Refresh	Refresh the current page.
13	Settings	<p>General:</p> <ul style="list-style-type: none"> <li>• Show files and folders of my PC: Set to show/hide files and folders on the local PC. This allows you to see the contents of your PC in File Station. This feature is currently only available in Windows and requires Java to be installed (you can download it from <a href="http://java.com">http://java.com</a>)</li> <li>• Show hidden files on QGW series: Set to show/hide hidden files.</li> <li>• Allow all users to create shared links.</li> <li>• Support multimedia playback and thumbnail display: If this option is checked, the file icon will be displayed as thumbnails.</li> <li>• Show Network Recycle Bin(s): Set to show/hide the "@Recycle" folder.</li> <li>• Only allow the admin and administrators group to use "Share to NAS user".</li> <li>• Only allow the admin and administrators group to permanently delete files: Check this option and 1) only administrators can permanently delete files from File Station; and 2) files deleted by other users will be moved to the Trash.</li> <li>• Remote connection: Configure the groups of users (administrators, administrators group, or specific users) that are allowed to use the Remote Connection feature.</li> </ul>
14	Help	Review the online help and check the About information.
15	Right Panel	Show/Hide the right panel.

**Tip:** If you are using Google Chrome, you can drag & drop files from your PC to File Station. However, some computers may not be able to upload files that are larger than 1GB using this method due to their low performance. When this happens, please consider uploading using File Station.

**Note:**

To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.

Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".

Only MP4 video files can be directly streamed if your QGW series does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, please refer to the [Transcode Management](#) chapter.

If your QGW series supports transcoding, please install the CodexPack App before using this function. The QGW series will try to transcode to a suitable format for your device. If your QGW series does not support transcoding, the QGW series will only output the original file format and the seek function may not work properly. In this case, please make sure that your device is compatible with the file format used by the video.

Some video formats may experience issues when streaming via DLNA, Apple TV or Chromecast. If any of these issues arise during video playback, you can consider transcoding your videos into universally-compatible media formats. For more details on transcoding, please refer to the [Transcode Management](#) chapter.

Some media players do not support pausing during playback. If this happens, playback will continue even if you use the pause feature.

For multimedia files transcoded using on-the-fly Transcoding, the time displayed on the media player seek bar will become 00:00 while you forward or rewind the multimedia files during playback.

The original photo files will be used for streaming if their thumbnails are not available.

**Left Panel**

- Volume: Every shared folder and folder on the QGW series is listed here. Depending on your QGW model, the default shared folders are different and can include "Download", "homes", "Multimedia", "Public", "Recordings", "USB" and "Web". You can click "+" next to a volume to create a shared folder on the volume.
- Local folders: Folders on your local PC are listed here. The Java JRE must be installed to use this feature.
- Favorites: Bookmarked folders are listed here.
- Qsync: Folders or files synchronized from the Qsync service are listed here.
- Share Link: Links of files shared from the QGW series are listed here.
- Share with me: Files and folders that have been shared to you from other QGW system users are listed here.

- Recycle Bin: Deleted files or folders can be found here. Right click on deleted items in the recycle bin to permanently delete or recover them.

### Right Panel

- Properties: Click this tab to review file and folder details, click "Calculate Size" to calculate the size of a folder, set the media type for the folder, and configure auto transcoding settings for the folder.
- Permission: Click this tab to configure shared folder permissions. For steps on setting folder permissions, please refer to the below "Set file/folder level permission" section.

### Using File Station

#### Creating shared folders

To create a shared folder, click "+" next to a volume, specify the folder name, folder description, disk volume, user access privileges, and advanced settings in the shared folder creation dialog window and click "Create".

#### Subfolder operations

Right click on a subfolder and choose to perform the following actions:

Action	Description
Sort By	Sort all the subfolders and files within the page by name, modified date, type, or size.
Create folder	Create a subfolder.
Copy/Paste	Copy a subfolder and paste it into another shared folder.
Share	<ul style="list-style-type: none"> <li>• Share the selected folder via email;</li> <li>• Publish the selected folder on social networks;</li> <li>• Set sharing details</li> </ul>
Open	Enter the chosen subfolder.
Download	Compress and download the subfolder.
Rename	Rename the subfolder.
Move	Move the subfolder to another location on the QGW series.
Delete	Delete the subfolder.
Cut/Paste	Cut a subfolder and paste it to another shared folder.
Add to Transcode (Beta)	Create transcode tasks for the files within the subfolder. If you see certain resolution options disabled in the "Add to

	Transcode(Beta)" window, it means the selected video files have already been transcoded into these resolutions.
Cancel/Delete Transcoding	Cancel / Delete transcode tasks created for the subfolder
Transcode Information	Bring up the Transcode Task window for your review on transcode tasks.
Add to Favorites	Bookmark the subfolder and it will appear under "Favorites" in the left panel.
Compress(Zip)	Compress the subfolder.
Properties	Switch to open the right panel.

**Tip:** For folders and files, the shortcut keys are provided for quick file and folder operations. Available shortcut keys include:

- Ctrl + C: Copy selected files/folders.
- Ctrl + V: Paste selected files/folders.
- Ctrl + X: Cut selected files/folders.
- Ctrl + A: Select all files/folders.
- Del: Delete selected files/folders.
- F2: Rename the selected file/folder.
- F5: Reload the current list.

## File operations

Right click on a file and choose to perform the following actions:

Action	Description
Sort By	Sort all the subfolders and files within the page by name, modified date, type, or size.
Copy/Paste	Copy a subfolder and paste it to another shared folder.
Share	Share selected files/folders via email, social network, by shared links, or to other QGW users. Refer to the <a href="#">Sharing files</a> section for more details.
View in Office Online	Open Office files stored on the QGW series using Office Online. The document will be first uploaded to Office Online and opened in a new browser tab. You must first install and sign in to the myQNAPcloud App to use this function.
View in Google Docs	Open Office files stored on the QGW series using Google Docs. The

	document will be first uploaded to Office Online and opened in a new browser tab. You must first install and sign in to the myQNAPcloud App to use this function.
Open with Chrome Extension	Preview and edit Microsoft Office files offline with a Chrome browser extension (Chrome only and requires the "Office Editing for Docs, Sheets & Slides" Chrome extension to be installed.)
Streaming to (Network Media Player)	Stream multimedia files (videos, music, and photos) to compatible devices in different rooms over your home network.
Play	Launch the Media Viewer and play the selected item.
Open	Open the file with a corresponding application on your PC. If no such applications are available, the file will be downloaded instead.
Open with VLC	If the chosen file is a video file, it will be opened in the browser (the VLC plug-in needs to be installed first.)
Download	Download the file. If the chosen file is a video that has been transcoded, you can choose its resolution and download the file. If multiple files are selected for download, they will be compressed before the download.
Rename	Rename the file.
Move	Move the file to another location on the QGW series.
Delete	Delete the file.
Cut/Paste	Cut a file and paste it to another shared folder.
Add to Transcode(Beta)	Create a transcode task for the file. Create transcode tasks for files within the subfolder. If you see certain resolution options disabled in the "Add to Transcode(Beta)" window, it means the selected video files have already been transcoded into these resolutions.
Cancel/Delete Transcoding	Cancel/Delete transcode task.
Transcode Information	Bring up the Transcode Task window for you to review transcode tasks.
Extract	Extract the compressed file.
Compress(Zip)	Compress the file.
Mount ISO	Mount the iso image as a shared folder on the left panel. After the file is mounted, you can click that shared folder to access the content of that iso image. To unmount an iso file, right click on the iso-mounted

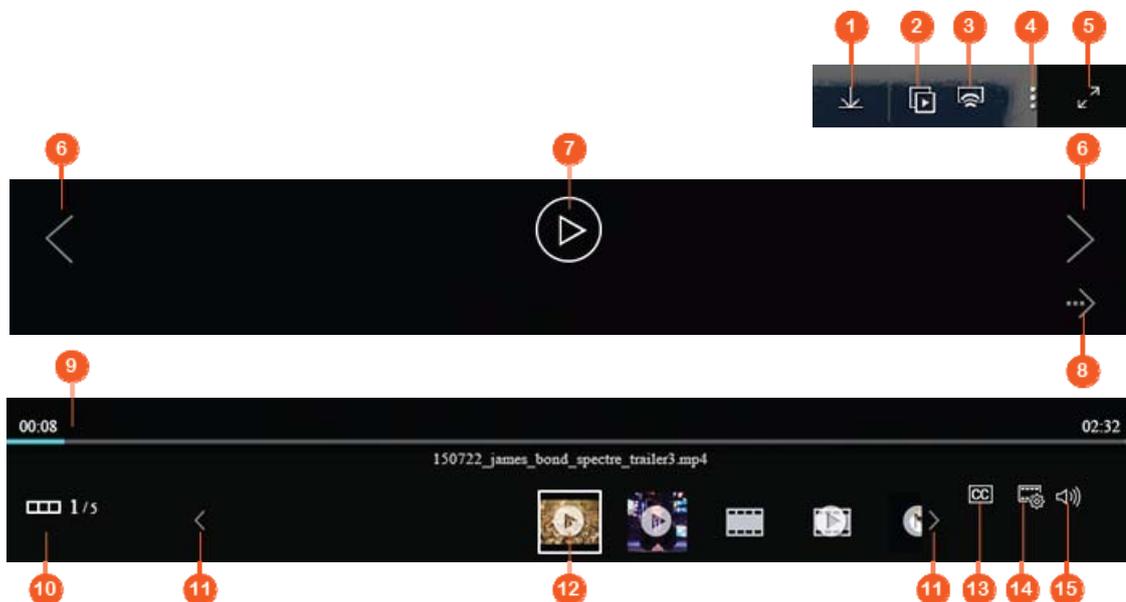
	shared folder in the left panel and choose "Unmount".
Properties	Switch to open the right panel.

**Note:**

- For IE 8, the maximum size of a file that can be uploaded to the QGW series by File Station is 2GB if the Java plug-in is not installed. We recommend using a modern web browser to access File Station.
- Due to limitations with Google Chrome, when using the upload folder function of the File Station toolbar only folders that contain at least one file can be uploaded. You can use drag & drop to circumvent this limitation.
- For Chrome, multiple files and folders can be dragged & dropped into File Station to upload them directly.
- For Mac OSX, mounting a folder that contains the # character in the folder name through WebDAV is not supported. Please rename the folder before mounting it if necessary.
- You can preview Microsoft Office files using File Station. To do so on Mac OSX, mounting a folder that contains the # character in the folder name through WebDAV is not supported. Please rename the folder before mounting it if necessary.
- For "View in Office Online" and "View in Google Docs", please set your browser to allow pop-ups and you will need a myQNAPcloud account. Supported file formats: .doc, .docx, .xls, .xlsx, .ppt, and .pptx.
- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW system does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable.

**Playing media files**

To play media files with File Station, double click on a multimedia file (photo, music and video files) and the Media Viewer (a built-in media player on the QGW series) will open to play the file. Use the following buttons to control the Media Viewer:



No	Name	Description
1	Download	Download the item.
2	Slideshow	Play all chosen photos as a slideshow. You can adjust the speed and effect of the slideshow (for photos only.)
3	Network Media Player	Stream videos to compatible devices in different rooms over your home network.
4	More Action	Rotate the photo, set the photo as the QTS Gateway the wallpaper, or delete the photo/video.
5	Full Screen	Switch to full screen mode.
6	Previous Item/Next Item	Play the previous/next item.
7	Play/Pause (videos)	Play/Pause the video.
8	Play/Pause (photos)	Play/Pause photos as slideshow.
9	Seek Bar	Control the playback progress.
10	Show/Hide Preview Bar	Hide/show the preview bar.
11	Last Item/Next Item	Play the last/next item on the preview bar.
12	Preview Bar	Preview the items in queue.
13	Subtitle	Manage subtitles of the video.
14	Resolution	Change resolution and transcoding settings.
15	Volume	Adjust the volume.

**Note:**

- The media viewer can be used to play photos and music files on all QGW series models. However, the feature to play videos using the media viewer is available on QGW series models that support hardware-accelerated transcoding.
- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW series does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, please refer to the [Transcode Management](#) chapter.
- Before enabling subtitles, please save the subtitles file (.srt format) in the same folder as the video file and ensure its name is the same as the video file.

**Finding your files/folders quickly**

File Station supports smart searching for files, sub-folders, and folders on the QGW series. You can search for files or folders using all or part of the file/folder name, by file type, or by file extension. There are two additional approaches you can quickly find your files: 1) advanced search and 2) smart file filter.

- For the advanced search, first click on the magnifier in the search bar and then "Advanced Search". Specify the search conditions (including name, size, date files are modified, location, type and owner/group) and click "Search". The files that match these conditions in the current folder will be listed.
- For the smart file filter, click on "Smart File Filter" in the Main Menu. Specify the filtering conditions (including name, size, date files are modified, type and owner/group) and click "OK". Files that match the conditions will be listed for the folder. This is the case even if you switch to a different folder.

**Note:** To search across all folders on the QGW series, click the drop down list in "Location" and select "...".

**Setting file/folder level permission**

You can set file or folder level permissions on the QGW series using File Station. Right click on a file/folder and select "Properties".

If "Advanced Folder Permissions" is disabled in "Privilege Settings" > "Shared Folder" > "Advanced Permissions", the following settings will be shown. Define the Read, Write, and Execute access rights for Owner, Group, and Others.

- Owner: Owner of file or folder.
- Group: Group owner of the file or folder.
- Others: Any other (local or domain member) users who are not the owner or a member of the group owner.

If a folder is selected, you can choose "Apply changes to folder(s), subfolder(s) and file(s)" to apply the settings to all the files and subfolders within the selected folder. Click "OK" to confirm.

If the "Enable Advanced Folder Permissions" option is enabled in "Privilege Settings" > "Shared Folder" > "Advanced Permissions", you will be able to specify the file and folder permissions by users and user groups. Click + to do so.

To select users and user groups and specify the Read and Write permissions, click "Add".

To remove permissions on the list, select the users or user groups and click "-".

You can also define the file and folder owner by clicking the edit button next to the owner field. To do this, select a user from the list or search for a username, and then, click "Set".

The following options are available for folder permission settings. It is recommended to configure folder permissions and subfolder permissions in "Privilege Settings" > "Shared Folders".

- Only the owner can delete the contents: When you apply this option to a folder, the first-level subfolders and files can only be deleted by their owner.
- Only admin can create files and folders: When you apply this option to a folder, only administrators can create files or folders.
- Apply changes to files and subfolders: Apply changed permissions settings except owner protection to all the files and subfolders within the selected folder. The option "Only the owner can delete the contents" will not be applied to subfolders.
- Apply and replace all existing permissions of this folder, files, and subfolders: Select this option to override all previously configured permissions of the selected folder and its files and subfolders except owner protection. The option "Only the owner can delete the contents" will not be applied to subfolders.

## Sharing files

To share files on the QGW series using File Station, right click on the files/folders and select "Share".

There are four sharing methods:

- Via email: Enter the required fields (including mail server from QGW series or local computer, sender, recipient, subject, message, domain name/IP and link name), choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Finally, preview the settings or directly share the file.

**Note: To share files/folders using your own email account, your email account must be set up in QTS Gateway Desktop > "Options" > "E-mail Account".**

- To social networks: Enter the required fields (including the social network to share the file, post message, domain name/IP and link name) choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings".

- Create share links only (generate a link to provide on instant messengers or store for later use): Complete required files (domain name/IP and link name), choose to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings".
- To QGW series users: Choose to share with new or existing QGW series users.
  - For new QGW series users, fill out account details (username and password), choose to allocate the quote, choose whether to send an email notification (and fill out message subject and content), set domain name/IP, link name and password for the link, decide whether to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Click "Preview" to preview the message or "Share Now".
  - For existing users, select existing user account(s), choose whether to send a notification email to the user (and fill out message subject and content), set domain name/IP, link name and password for the link, decide whether to include SSL (https://) in the URL, and optionally set an expiration time and password in "More settings" . Click "Preview" to preview the message or "Share Now".

For folders, there will be an option "Allow file upload to this folder" in the dialog window for all four sharing options. This feature is only for administrators and can allow link recipients to upload files to the folder pointed to by the link.

For the "To NAS users" option, if you choose to share with new users, the system will create new user accounts. Also, the email recipients (or users you share files with) can check files shared in File Station > "Share with me" on the left panel after they log into the QGW series.

### **Sharing space**

Administrators can allocate space to QGW series users and specify a storage quota in File Station by following these steps:

1. Click "Create" (the "+" icon) on the Menu Bar > "Share space with a user".
2. Complete the required fields in the "Create a User" page.
3. Enable the quote feature and set the quota size in "Control Panel" > "Privilege Settings" > Quote" if you have not already done so.
4. Specify the email (optional) and phone number (optional) for the user.
5. Choose to send an email notification to the newly-created user (optional), fill out the message details (including mail server (from QGW series or local computer), sender, recipient, subject, message, domain name/IP and link name) and choose to include SSL (https://) in the URL.
6. Click "Create".

## Remote Connection

The remote connection service allows you to easily manage files across local devices, external devices, cloud services and remote devices from a single interface. You can easily carry out file management tasks such as copying and moving from remote to local devices or vice versa. The remote connection service supports multiple cloud services (such as Google Drive, Dropbox, and OneDrive) and remote device network protocols (such as CIFS/SMB, FTP and WebDAV.)

### Create remote connections

1. Click the "Remote Connection" button on the "Menu Bar" > "Create remote connection".
2. Choose to connect to a remote storage via SMB/CIFS, FTP, or WebDAV.
3. Fill out necessary details (including the protocol, codepage, hostname/IP, username/password, destination folder and connection name) and choose to enable support for multimedia playback and thumbnail display (the system will generate thumbnails at the destination; if the destination is another QGW series system, it must have QTS Gateway 4.2 or above installed)
4. Click "Create".

### Check recent connection records

1. Click the "Remote Connection" button on the "Menu Bar" > "Connection record".
2. Review recent connection records and their details including the connection time, connection name, protocol, Hostname/IP, port, account username, codepage and source path.
3. To sort the records, click on a header.

### Check the current connection status

1. Click the "Remote Connection" button on the "Menu Bar" > "Current connection status".
2. Review the status of the current connections records and their details, including the connection time, connection name, protocol, Hostname/IP, port, account username, codepage and source path.
3. To sort records, click on a header.

#### **Note:**

- For Remote Connection, the maximum number of connections that can be created per QGW system is 256.
- OneDrive for Business is not supported for Remote Connection.
- To share links by email, the email server settings must be properly configured in "System Settings" > "Notification" > "SMTP Server".
- Up to 1000 sharing links are supported.
- For best performance, use one of the following browsers: IE 9+, Firefox 3.6+, Safari 5+, or Chrome.

- Do not close the browser before the file transfer process (upload or download) is completed or the process will fail.
- For Remote Connections, you must install the Connect to Cloud Drive app from the App Center before connecting to cloud services.
- Using a remote connection is identical to an external device and ongoing tasks will be terminated if the QGW series is restarted or powered off.
- Limitations of your cloud service account may affect what files can be transferred. Please check the account details with your cloud service providers for more information regarding what files can and cannot be transferred.
- When transferring a large amount of files over CIFS/SMB using a remote connection, some antivirus software may cause the transfer to fail. If you encounter this problem, please temporarily disable your antivirus software and try again.
- Due to performance limitations of web browsers and PCs, you may not be able to upload a large amount of files in one task. If you encounter this problem, please separate your upload task into multiple tasks or use another upload method.

# LDAP Server

The LDAP server of the QGW series allows the administrator to create users to access multiple QGW series systems with the same username and password.

LDAP Server

Enable LDAP Server

Full domain name:

Password:

Verify password:

Root DN: cn=admin,dc=my-domain,dc=com

Users base DN: ou=people,dc=my-domain,dc=com

Group base DN: ou=group,dc=my-domain,dc=com

Initialize LDAP database:  (Delete all users and groups from the LDAP server)

Enable this NAS to be the client of the LDAP service: [Domain Security](#)

## Configuring LDAP Server

Follow these instructions to configure the LDAP server.

1. Enable LDAP Server: Login to the QGW series as "admin". Go to "Applications" > "LDAP Server" and enable the LDAP server. Enter the full LDAP domain name and the password for the LDAP server, then click "Apply".
2. Create LDAP Users: Under the "Users" tab, click "Create a User" or "Create Multiple Users" or "Batch Import Users". Follow the wizard instructions to create LDAP users. Once you have created the LDAP users, the QGW series can be joined to the domain. You can set the permissions of LDAP users and allow them to be authenticated by the QGW series.
3. Join a QGW system to LDAP Domain: To allow LDAP users to connect to the QGW series, join the QGW series to the LDAP domain. Go to "Privilege Settings" > "Domain Security". Select "LDAP authentication" and choose "LDAP server of local NAS" as the server type. Then click "Apply". The QGW series is now a client of the LDAP server. To view the domain users or groups, go to "Privilege Settings" > "Users" or "User Groups", then select "Domain Users" or "Domain Groups". You can also set the folder permission for the domain users or groups.
4. Join a Second QGW system to LDAP Domain: You can join multiple QGW systems to the same LDAP domain and allow the LDAP users to connect to these QGW systems using the

same login credentials. To join another QGW system to the LDAP domain, login to the QGW system and go to "Privilege Settings" > "Domain Security", select "LDAP authentication" and set "LDAP server of a remote NAS" as the server type. Enter the DNS name or IP address of the remote QGW system, the name of the previously-created LDAP domain, and enter the LDAP server password. Click "Apply".

### **Backing up/Restoring LDAP Database**

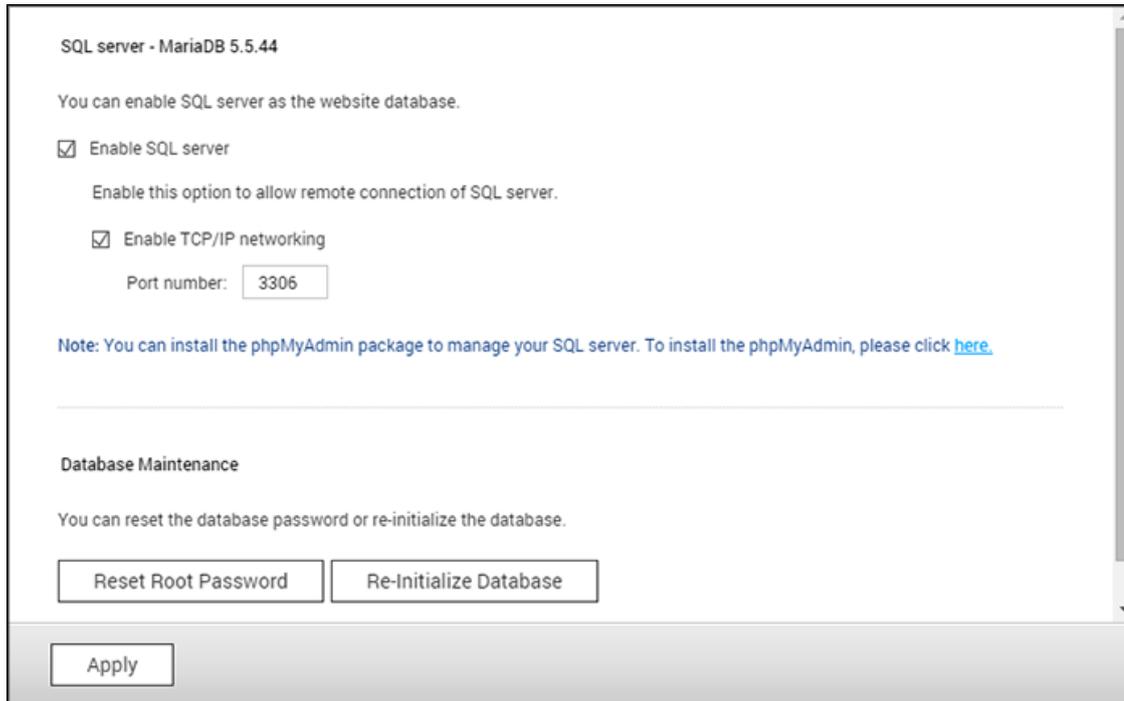
To back up the LDAP database on the QGW series, select "Back up Database" and specify the backup frequency, destination folder on the QGW system and other options. To restore an LDAP database, browse to select the \*.exp file and click "Import".

#### **Note:**

- If the name of a user is changed in a LDAP server, it is necessary to assign the folder permissions again on the QGW system.
- To avoid account conflicts, do not create local user accounts that already exist in the LDAP directory.

# SQL Server

You can enable an SQL Server to be a website database.



SQL server - MariaDB 5.5.44

You can enable SQL server as the website database.

Enable SQL server

Enable this option to allow remote connection of SQL server.

Enable TCP/IP networking

Port number:

Note: You can install the phpMyAdmin package to manage your SQL server. To install the phpMyAdmin, please click [here](#).

---

Database Maintenance

You can reset the database password or re-initialize the database.

## Enable TCP/IP Networking

You can enable this option to configure MySQL server of the QGW system as a database server of another web server in remote site through Internet connection. If this option is disabled, your MySQL server will only be configured as a local database server for the web server of the QGW system. After enabling remote connection, assign a port for the remote connection service of the MySQL server. The default port is 3306. After the first-time installation of the QGW system, a phpMyAdmin folder is created in the Qweb/Web network folder. You can enter `http://QGW IP/phpMyAdmin/` in the web browser to enter the phpMyAdmin page and manage the MySQL database.

## Database Maintenance

- Reset root password: Reset the password of MySQL root as "admin".
- Re-initialize database: Delete all the data on the MySQL database.

### Note:

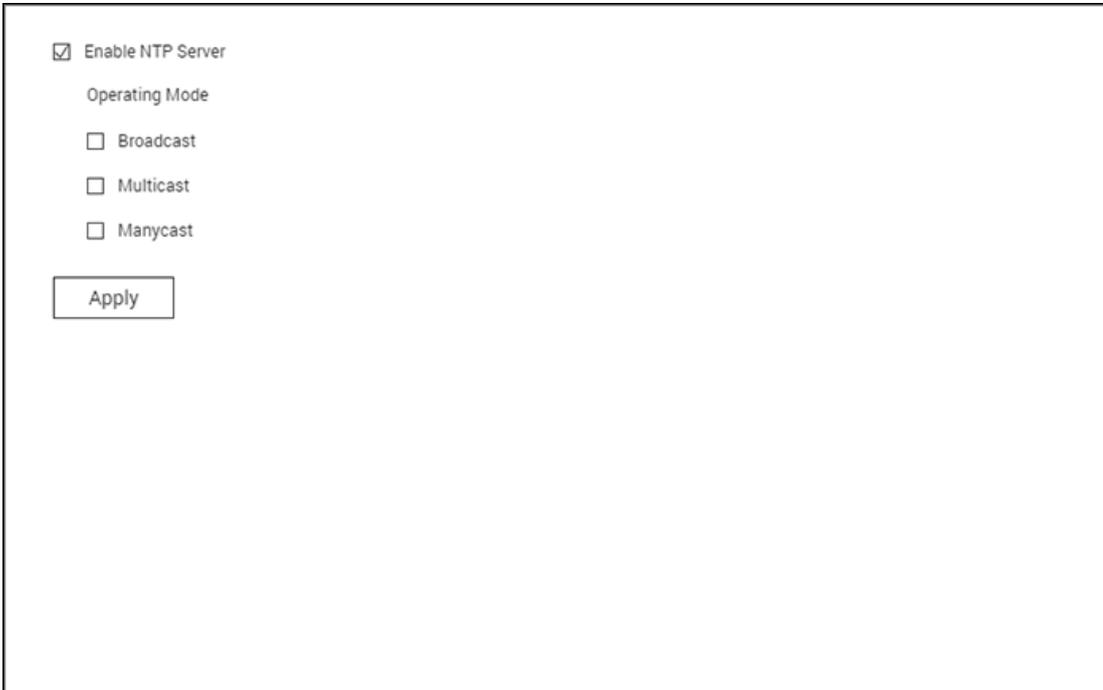
- Do not delete the phpMyAdmin folder. You can rename the folder but the link on the MySQL server page will not be updated. To connect to the renamed folder, you can

enter the link [http://QGW IP/renamed folder](http://QGW_IP/renamed_folder) in the web browser.

- The phpMyAdmin folder is created after the first-time installation. When you update the firmware, the folder will remain unchanged.

# NTP Service

A NTP Server allows the PCs, servers and other network devices to synchronize their time with the same reference: the QGW system. It is useful (and sometimes required) to keep the time synchronized for all devices in some environments.



The screenshot shows a configuration window for the NTP Service. It features a checked checkbox labeled "Enable NTP Server". Below this, under the heading "Operating Mode", there are three unchecked checkboxes: "Broadcast", "Multicast", and "Manycast". At the bottom left of the window is an "Apply" button.

## Setting up NTP Server

To set up the NTP Server, first go to "Control Panel" > "Applications" > "NTP Service" and check "Enable NTP Server". Select to check the following three operating modes:

- **Broadcast:** This will allow the NTP server to periodically send broadcast packets with the IP address "255.255.255.255 ". Clients compatible with this mode can use this to synchronize their time.
- **Multicast:** This will allow the NTP server to periodically send multicast packets. Clients compatible with this mode can use this to synchronize their time. Specify the multicast IP address after this option is enabled.
- **Manycast:** This will allow the NTP server to listen for manycast requests from NTP clients and reply to the client requests received. Specify the manycast address after this option is enabled.

**Note:** For multicast and manycast modes, the NTP clients will only receive this kind of packets after they are configured for the modes. Please refer to their user manuals for setup details.

# RADIUS Server

The QGW system can be configured as a RADIUS (Remote Authentication Dial In User Service) server to provide centralized authentication, authorization, accounting management for computers to connect and use a network service.

The screenshot shows a web interface for configuring the RADIUS server. At the top, there are three tabs: "Server Settings", "RADIUS Clients", and "RADIUS Users". The "Server Settings" tab is active. Below the tabs, there are two checked checkboxes: "Enable RADIUS Server" and "Grant dial-in access to system user accounts". A blue note below the checkboxes reads: "Note: RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication schemes for system user accounts." Below the note is an "Apply" button. At the bottom of the interface, there is an "Apply All" button.

To use this feature, follow these steps:

1. Enable RADIUS Server on the QGW series in "RADIUS Server" > "Server Settings". Click "Apply".
2. Add RADIUS clients, such as Wi-Fi access points and VPN, on the QGW series in "RADIUS Server" > "RADIUS Clients". Up to 10 RADIUS clients are supported. Click "Create a Client".
3. Enter the client information and click "Apply".
4. The clients are shown on the list.
5. Create RADIUS users and their password in "RADIUS Server" > "RADIUS Users". The users will be authenticated when trying to access the network through RADIUS clients. The maximum number of RADIUS users the QGW series supports is the same as the maximum number of local QGW users supported. See the chapter on [Users](#) for details. Click "Create a User".
6. Enter the username and password. The username only supports letters (a-z and A-Z) and numbers (0-9). The password must be 8-32 characters in length.
7. Specify to grant dial-in access to local QGW users. Enable this option to allow local QGW users to access network services via RADIUS clients using their QGW series login name and password.

**Note:** The RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication for local QGW user accounts.

# Syslog Server

Configure the QGW series as a Syslog server, create Syslog filters and view available Syslog messages on this page.

The screenshot shows the configuration page for the Syslog Server. It is divided into two main sections: 'Server Settings' and 'Log Settings'. In the 'Server Settings' section, the 'Enable Syslog Server' checkbox is checked. Below it, the 'Enable TCP' checkbox is also checked, with a 'TCP port' input field set to '514'. Similarly, the 'Enable UDP' checkbox is checked, with a 'UDP port' input field set to '514'. The 'Log Settings' section includes a 'Maximum log size (MB)' input field set to '50'. The 'Log file' field is configured with a dropdown menu set to 'Download' and a text input field containing 'messages'. An 'Apply All' button is located at the bottom of the configuration area.

## Server Settings

- **Server Settings:** To configure the QGW series as a Syslog server and allow it to receive Syslog messages from clients, enable Syslog Server. Select the protocols (TCP and/or UDP) the QGW series uses to receive Syslog messages. Specify the port numbers if necessary or use the default port number 514. Click "Apply" to save the settings. After enabling the QGW series as a Syslog server, enter the QGW system IP as the Syslog server IP on the Syslog clients to receive Syslog messages from them.
- **Log Settings:** Specify the maximum log size (1-100 MB) of Syslog messages, the location (QGW shared folder) where the logs will be saved, and the file name. Once the logs have reached their maximum size, the log file will be automatically archived and renamed with the archive date as MyLogFile\_YYYY\_MM\_DD, for example MyLogFile\_2011\_12\_31. If multiple log files are archived on the same day, the file will be named as MyLogFile\_YYYY\_MM\_DD.[number]. For example, MyLogFile\_2011\_12\_31.1, MyLogFile\_2011\_12\_31.2, and so on. Click "Apply" to save the settings.
- **Email Notification:** The QGW series supports sending email alerts to up to 2 dedicated email addresses (configured in "System Settings" > "Notification" > "Alert Notification") when the severity of the received Syslog messages match the specified level. To use this feature, configure the SMTP server settings in "System Settings" > "Notification" >

"SMTP Server". Next, enable email notification and select the severity level in "Applications" > "Syslog Server" > "Server Settings". Click "Apply" to save the settings.

Severity	Level (smallest number the highest)	Description
Emerg	0	Emergency: the system is unusable. Alert emails will be sent when Syslog messages of levels 0-4 are received.
Alert	1	Alert: immediate action required. Alert emails will be sent when Syslog messages of levels 1-4 are received.
Crit	2	Critical: critical conditions. Alert emails will be sent when Syslog messages of levels 2-4 are received.
Err	3	Error: error conditions. Alert emails will be sent when Syslog messages of levels 3-4 are received.
Warning	4	Warning: warning conditions. Alert emails will be sent when Syslog messages of level 4 are received.

## Filter Settings

This feature should only be operated by administrators who are familiar with Syslog filters. Follow these steps to create Syslog filters for the QGW series to receive Syslog messages that match the criteria:

1. Click "Add a Filter".
2. Define the filter settings and click "Add". To edit the filters or to manually add filters, click "Manual Edit" and modify the contents in the dialog. Click "Apply" to save the filter.
3. The filters will be shown on the list. The QGW series will only receive Syslog messages that match the filters which are in use.

Button	Name	Description
	Enable	Enable a filter
	Disable	Disable a filter

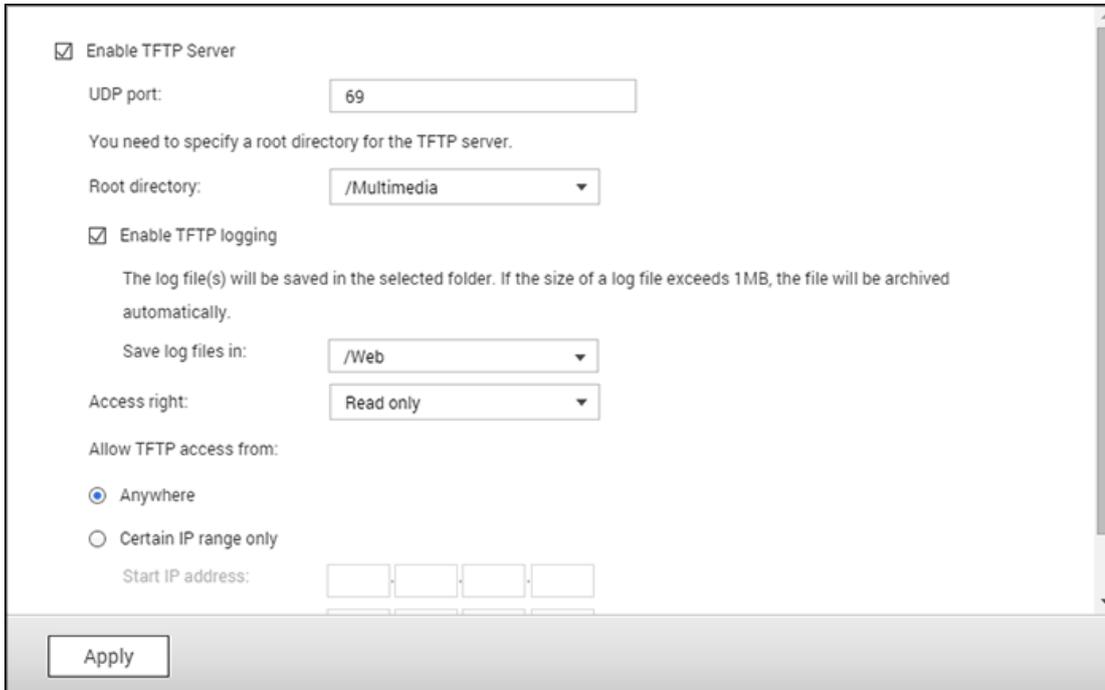
	Edit	Edit filter settings
Delete	Delete	Delete filters

## Syslog Viewer

Use the Syslog viewer to view the available Syslog messages on the QGW series. Select to view the latest logs or the logs in a particular archived file. Log files can be accessed on the directory configured in "Syslog Server" > "Server Settings" > "Log Settings".

# TFTP Server

Configure the QGW series as a TFTP (Trivial File Transfer Protocol) server for configuration management of network devices and remote network booting of computers for system imaging or recovery. TFTP is a file transfer protocol with the functionality of a very basic form of FTP. TFTP does not provide user authentication and cannot be connected to using a standard FTP client.



Follow these steps to use this feature:

1. Select "Enable TFTP Server".
2. The default UDP port for file transfer is 69 and you should only change it if necessary.
3. Specify a folder on the QGW series as the root directory of the TFTP server.
4. Enable TFTP Logging: Enable this option and specify the directory to save the TFTP log file (opentftpd.log.) It is recommended to view the log file using Microsoft Excel or WordPad on Windows OS or by TextEdit on Mac OS.
5. Assign read only or full access to the clients.
6. Restrict the TFTP client access by specifying the IP address range or select "Anywhere" to allow any TFTP client access.
7. Click "Apply".

**Note:** To set up PXE with your QGW series, please use a static IP for your QGW series, enable its DHCP service and specify the TFTP server IP and name of the boot file in "Control Panel" > "Network" > click the "Edit" button next to the LAN port > "DHCP server". For more details, please refer to the [DHCP Server](#) chapter

# Virtualization

IEI QGW series is a virtualization-ready storage solution designed to optimize your virtualization operations. In addition to the support for VMware vSphere, Microsoft Hyper-V and Citrix XenServer, this storage solution includes the cutting edge VAAI and ODX (Offloaded Data Transfer) technologies to offload the heavy-duty file operations from the servers and flexible volume management approaches, such as Thin Provisioning and Space Reclaim, to manage your volumes more effectively. To double system performance, IEI offers a number of network accessories that support 10Gbe transmission speeds and the SSD Cache feature that capitalizes on SSD technologies. Besides, the remarkable vSphere Client and SMI-S Provider are available to increase management productivity and efficiency.

## Server Virtualization

The QGW series supports three types of server virtualization applications: VMware vSphere, Microsoft Hyper-V and Citrix XenServer.

### VAAI for QGW Series

The QGW series supports VMware VAAI (vStorage APIs for Array Integration) to increase operational performance in virtualization environments. With VAAI, data processing is offloaded to the QGW series, and standard virtual machine management and deployment can be performed more efficiently, consuming less ESXi CPU, memory, and bandwidth resources.

VAAI for QGW series offers the following three features:

- **Full File Clone:** Enables the QGW series to copy all data within the QGW series without requiring that the ESXi host reads and writes the data. This feature can reduce loading for ESXi hosts, speeds up the cloning process for virtual machines.
- **Extended Statistics:** Enables vSphere to query space utilization details for virtual disks on NFS datastores, including the size of a virtual disk and the real space consumption of that virtual disk. This feature can report disk space consumption more accurately, increase storage space utilization and save IT cost.
- **Reserve Space:** Reserves the pre-allocated space of virtual disks (thick provision eager zeroed disks) in NFS datastores. This feature can increase virtual disk read/write performance (thin provision disks vs. thick provision disks.)

With the support of VAAI for QGW series, the QGW series can boost storage performance (more than 120 times faster) to create new virtual machines in a virtualized environment.

### **SSD Cache**

Based on the SSD technology, the SSD cache feature is designed to boost access performance of the QGW series. As the name "SSD Cache" implies, SSD drives need to be installed to enable this function.

### **vSphere Client**

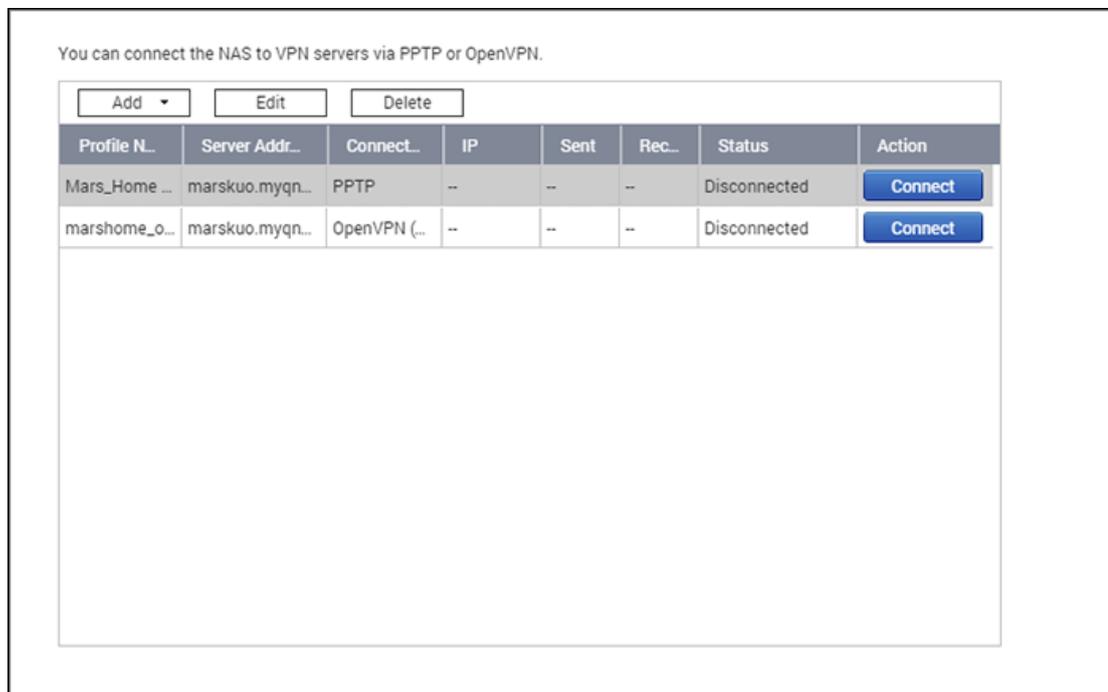
The vSphere Client for QGW series is an interface between ESXi and the QGW series. This tool allows system administrators to manage VMware datastores on the QGW series directly from the vSphere Client console and verify the status of all QGW series units.

### **SMI-S Provider**

SMI-S Provider is a required component for the support of System Center Virtual Machine Manager (SCVMM 2012). With this tool, the QGW series can directly communicate with SCVMM 2012, and server management tasks can be facilitated for administrators.

# VPN Client

The QGW series provides the VPN client service which can connect to a VPN server via PPTP or OpenVPN. The QGW series also supports saving multiple VPN settings to easily switch between different connections.



Topics covered in this chapter:

- [Before you Start](#)
- [Connect a VPN Server via PPTP](#)
- [Connect a VPN Server via OpenVPN](#)

## Before you start

Before starting the VPN client service, please ensure that your QGW series has been set up as follows:

- The Internet connection is normal.
- Your QTS Gateway version is at least 4.1.2.
- If you have an active VPN server service, you must disable it. The client and server services cannot run at the same time.

## Connect a VPN server via PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a commonly-used method for implementing VPN and is supported by most clients, including Windows, Mac OS X, Linux, and mobile devices.

1. Go to "Control Panel" > "VPN Client".
2. Click "Add" > "PPTP" to connect a VPN server.
3. Enter the connection configuration settings, including the profile name, server address (that you want to connect to), and the username and password of the VPN server.
4. Choose any of the following authentication mechanisms from the "Authentication" menu to protect VPN client's password during authentication:
  - o MS-CHAPv2: The password will be encrypted using Microsoft CHAP version 2.
  - o MS-CHAP: The password will be encrypted using Microsoft CHAP version 1.
  - o PAP: The password will not be encrypted.
  - o CHAP: The password will be encrypted using CHAP.
5. If you choose MS-CHAP or MS-CHAPv2, go to the "Encryption" menu and select an option:
  - o None: The VPN connection will not be encrypted.
  - o Medium (AES 40/128 bit): The VPN connection will be encrypted using a 40-bit or 128-bit key.
  - o High (AES 256 bit): The VPN connection will be encrypted using a 256-bit key (the highest-possible level.)
6. Tick the following checkboxes depending on your configurations:
  - o Use the default gateway on remote network: This will allow all packets to be transferred via the VPN server.
  - o Allow other network devices to connect to the VPN through the QGW series: This will allow network devices on the same LAN as the QGW series to connect to the same VPN.
  - o Reconnect when the VPN connection is lost: This will automatically reconnect to the VPN server when the connection is lost.
7. Select "Connect" to start.

**Note:** If you check "Use the default gateway on remote network", the default gateway on your QGW series will change to the VPN server's default gateway.

If you check "Allow other network devices to connect to the VPN through the NAS", the network device can access the VPN via the QGW series. To enable this function, you must change the default gateway on that other device. Using a Windows PC as an example:

1. Go to "Control Panel" > "Network a Sharing Center" > "Change adapter settings".
2. Right click on the connection icon and choose "Properties".
3. Select "Internet Protocol Version 4 (TCP/IP)" and click "Properties".
4. Choose "Use the following IP address" and change the Default gateway to the IP address of the QGW series that is operating the VPN Client service (in this case, it is 192.168.1.14) then click "OK".

## Connect a VPN server via OpenVPN

The QGW series also supports OpenVPN, which is an open-source solution for VPN services. It protects a VPN's connection with the SSL/TLS encrypting mechanism. It is also available on Windows, Mac OS X, Linux, Android and iOS.

To connect to a VPN server via OpenVPN, follow these steps:

1. Log into the QGW series and go to "Control Panel" > "Application" > "VPN Client" > click "Add" and choose "OpenVPN" to connect to a VPN server.
2. Enter the connection configuration settings, including the profile name, server address (that you want to connect to), and the username and password of the VPN server. Choose the same configuration as the OpenVPN server in "Server Port".
3. Click "Certification" to import the certificate (ca.crt) exported from the OpenVPN server.
4. Tick the following checkboxes depending on your configurations:
  - Enable compressed VPN link: This will compress data before transferring via VPN.
  - Use the default gateway on remote network: This will allow all packets to be transferred via the VPN server.
  - Allow other network devices to connect to the VPN through the QGW series: This will allow network devices on the same LAN as the QGW system to connect to the same VPN.
  - Reconnect when the VPN connection is lost: This will automatically reconnect to the VPN server when the connection is lost.
5. Click "Connect" to start.
  - If you check "Use the default gateway on remote network", the default gateway on your QGW series will change to the VPN server's default gateway.
  - If you check "Allow other network devices to connect to the VPN through the NAS", please refer to the above tutorial for more details.

# VPN Server

The QGW series supports Virtual Private Network (VPN) service for users to access the QGW series and resources on a private network from the Internet. Set your QGW series as a VPN server on this page.

VPN Server Settings   Privilege Settings   Connection List

**PPTP Settings**

The PPTP server allows users to access the LAN remotely. Use the default settings or specify the settings manually. To understand more, please check: <https://www.qnap.com/vpnserver>

Enable PPTP VPN server

VPN client IP pool: 10 . 0 . 0 . 2 - 10 . 0 . 0 . 254

Advanced Settings ▲

Maximum number of clients: 5 ▼

Authentication: MS-CHAPV2 ▼

Encryption: High (AES 128 bit) ▼

Network interface: Ethernet 1 ▼

Specify DNS server manually: 0 . 0 . 0 . 0

Apply All

In this chapter, the following topics are covered:

- [VPN Server Setup](#)
- [Third Party VPN Client Setup and Connection](#)
- [Privilege Settings](#)
- [Connection List](#)

## VPN Server Setup

1. Enable PPTP or OpenVPN service: The QGW series supports PPTP and OpenVPN for VPN connection. Select either one option and configure the settings.
  - PPTP: Point-to-Point Tunneling Protocol (PPTP) is one of the most commonly used methods for VPN connection. It is natively supported by Windows, Mac, Linux, Android, and iPhone. You can also specify the VPN client IP pool and advanced settings (including the maximum number of clients, authentication protocol, encryption method, network interface and DNS server.)
  - OpenVPN: OpenVPN is an open source VPN solution which utilizes SSL encryption for secure connection. To connect to the OpenVPN server, OpenVPN client must be installed on your PC. Click "Download Configuration File" to download the VPN client settings, certificate/key and installation guide from the QGW series and upload the

files to the OpenVPN client. You can also specify the VPN client IP pool and advanced settings (including the VPN server port, maximum number of clients, encryption method, network interface, DNS server, and whether to use the redirect-gateway and compressed data before their transfer via VPN.)

2. Configure port forwarding by auto router configuration: The QGW series supports auto port forwarding for UPnP (Universal Plug-and-Play network protocol) routers. Go to "myQNAPcloud" > "Auto Router Configuration" to enable UPnP port forwarding and open the ports of the PPTP or OpenVPN service on the router.
3. Register myQNAPcloud service: You can connect to the QGW series by WAN IP or myQNAPcloud name. To configure myQNAPcloud service, check the chapter on myQNAPcloud Service or visit [myQNAPcloud](https://www.myqnapcloud.com) (<https://www.myqnapcloud.com>).
4. Add VPN users: Go to "Applications" > "VPN Server" > "Privilege Settings", click "Add VPN Users". The local QGW users will be listed. Select the users who are allowed to use the VPN service and their connection method (PPTP, OpenVPN, or both). Click "Add".
  - o Connect to the private network by a VPN client: Now you can use your VPN client to connect to the QGW series via the VPN service.

**Note:**

- The default QGW system IP is 10.0.0.1 under PPTP VPN connection.
- Upload the configuration file to the OpenVPN client every time the OpenVPN settings, myQNAPcloud name, or the secure certificate is changed.
- To connect to the PPTP server on the Internet, the PPTP passthrough options on some routers have to be opened. PPTP uses only port TCP-1723; forward this port manually if your router does not support UPnP.

**Additional Reference:**

- You can add an extra layer of security to the VPN service by installing L2TP/IPsec from the App Center. Please refer to the [NAS Add-ons](#) chapter for details.

## Third Party VPN Client Setup and Connection

### PPTP on Windows 7

1. Go to "Control Panel" > "Network and Sharing Center". Select "Set up a new connection or network".
2. Select "Connect to a workplace" and click "Next".
3. Select "Use my Internet connection (VPN)".
4. Enter the myQNAPcloud name or the WAN IP of the QGW series and enter a name of the connection. Then click "Next".
5. Enter your username and password which is added from the QGW series for VPN access. Click "Connect".

### PPTP on Mac OS X 10.7

1. Choose "Apple menu" > "System Preferences", and click "Network".
2. Click "Add (+)" at the bottom of the list, and choose "VPN" as the interface.
3. Choose the VPN type according to the QGW series settings to connect. Enter the service name.
4. In "Server Address", enter the myQNAPcloud name or the WAN IP of the QGW series. In "Account Name", enter your username which is added from the QGW series.
5. Click "Authentication Settings", and enter the user authentication information given by the network administrator.
6. After entering the user authentication information, click "OK", and then click "Connect".

### PPTP on iOS 5

1. Go to "Settings" > "General" > "Network", select "VPN".
2. Select "Add VPN Configuration".
3. Select "PPTP", and enter the Description, Server, Account, and Password for the connection.
4. Return to "Settings" > "General" > "Network" > "VPN", and enable "VPN".

### OpenVPN on Windows

1. Download OpenVPN from <http://openvpn.net/>
2. Install the OpenVPN client on Windows. The default installation directory is C:\Program Files\OpenVPN.
3. Open OpenVPN as an administrator.
4. Download the OpenVPN configuration file and certificate from the QGW series ("Applications" > "VPN Server" > "VPN Server Settings" > "OpenVPN Settings")
5. Edit openvpn.ovpn and replace "OPENVPN\_SERVER\_IP" with the OpenVPN server IP.
6. Put "ca.crt" and "openvpn.ovpn" into the configuration folder under the OpenVPN configuration subdirectory (C:\Program Files\OpenVPN\config.)

**Note:** If the OpenVPN client is running on Windows 7, add the firewall rules in the advanced settings of OpenVPN.

### OpenVPN on Linux

1. Download OpenVPN from <http://openvpn.net/index.php>
2. Install the OpenVPN client on Linux.
3. Download the OpenVPN configuration file and certificate from the QGW series ("Applications" > "VPN Server" > "VPN Server Settings" > "OpenVPN Settings".)
4. Edit openvpn.ovpn and replace "OPENVPN\_SERVER\_IP" with the OpenVPN server IP.
5. Put "ca.crt" and "openvpn.ovpn" into the configuration folder under the OpenVPN configuration subdirectory.

6. Run OpenVPN.

### **OpenVPN on Mac**

1. Download the disk image of OpenVPN client from <http://code.google.com/p/tunnelblick/>
2. Launch Tunnelblick.
3. Download the OpenVPN configuration file and certificate from the QGW series ("Applications" > "VPN Service" > "VPN Server Settings" > "OpenVPN Settings".)
4. Edit openvpn.ovpn and replace OPENVPN\_SERVER\_IP (alfred.myqnapnas.com) with OpenVPN server IP.
5. Put "ca.crt" and "openvpn.ovpn" into the configuration folder under the OpenVPN configuration subdirectory.
6. Run OpenVPN.

### **Privilege Settings**

Select the VPN users and specify their privileges.

#### **Add VPN users**

Click "Add VPN Users" and follow the wizard to select the system users and set their privileges.

#### **Delete VPN users**

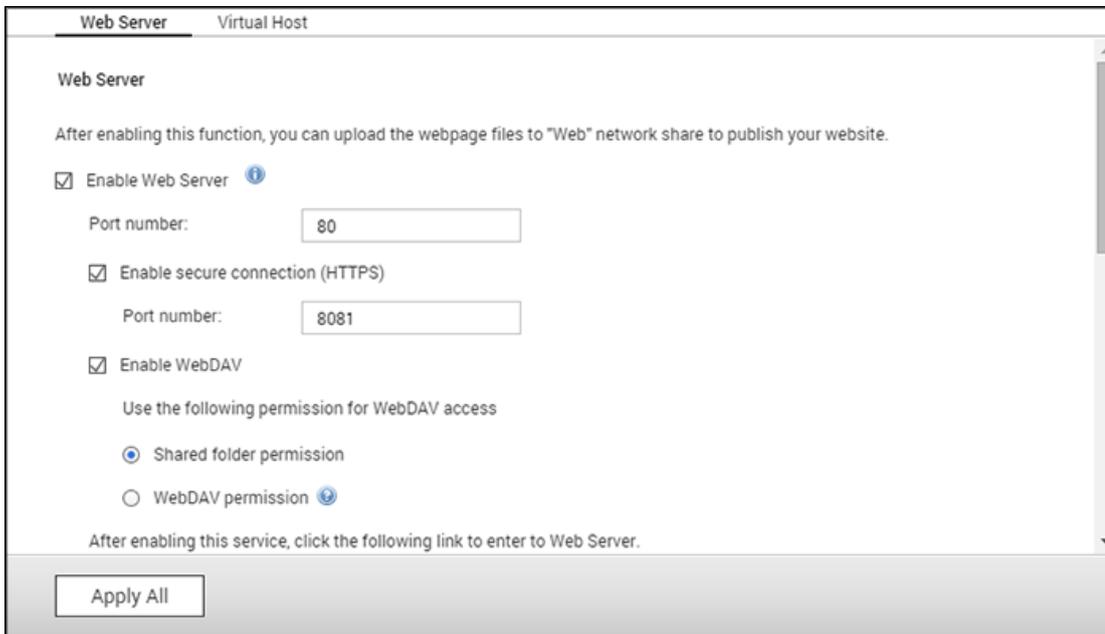
Click "Delete" to remove the VPN users. The users will not be able to connect to the VPN service after being deleted.

#### **Connection List**

This list shows the connection status of the VPN clients. You can right click a client on the list and select to disconnect the client.

# Web Server

Go to "Control Panel" > "Applications" > "Web Server" to configure the web server and virtual host.



## Web Server

The QGW series can host web sites including those that use Joomla!, PHP and MySQL/SQLite to establish an interactive website. To use the Web Server, follow these steps.

1. Enable the service and enter the port number. The default number is 80.
2. Configure other settings:
  - a. Maintenance: Click "Restore" to restore the web server configuration to default.
  - b. php.ini Maintenance: Choose to upload, edit or restore php.ini.
3. Secure Connection (SSL): Enter the port number for SSL connection.
4. Upload HTML files to the shared folder (Qweb/Web) on the QGW series. The file index.html, index.htm or index.php will be the home path of your web page.
5. You can access the web page you upload by entering http://QGW system IP/ in the web browser. When the Web Server is enabled, you must enter http:// QGW system IP:8080 in your web browser to access the QGW system login page.

### Note:

- If the Web Server is disabled, all relevant applications including Photo Station, Happy Get, or QAirplay will become unavailable.
- To use PHP mail(), go to "System Settings" > "Notification" > "SMTP Server" and configure the SMTP server settings.

## WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to the HTTP(S) protocol that allows users to edit and manage files collaboratively on remote servers. After enabling this function, you can map shared folders of your QGW system as network drives of a remote PC over the Internet. To edit the access rights, go to "Privilege Settings" > "Shared Folders" page.

**Note:** WebDAV currently supports QGW system user accounts and AD domain user accounts. LDAP user accounts are not supported.

To map a shared folder as a network drive on your PC, enable WebDAV and follow these steps.

1. Go to "Privilege Settings" > "Shared Folders". Click "Access Permissions" for the designated folder under the "Action" column.
2. Select "WebDAV access" from the dropdown menu on the top of the page and specify the access rights. Choose the authentication level or scroll down to search for the account to grant its access rights. Click "Apply".
3. Next, mount the QGW system shared folders as the shared folders on your computer using WebDAV.

## Windows Vista

If you are using Windows Vista, you may need to install "Software Update for Web Folders (KB907306)". This update is only for 32-bit versions of Windows Vista.

<http://www.microsoft.com/downloads/details.aspx?FamilyId=17c36612-632e-4c04-9382-987622ed1d64&displaylang=en>

1. Right click on "Computer" and select "Map Network Drive..."
2. Click "Connect to a Web site that you can use to store your documents and pictures".
3. Select "Choose a custom network location".
4. Enter the QGW system URL with the folder name. Format:  
http://QGW\_IP\_or\_HOST\_NAME/SHARE\_FOLDER\_NAME
5. Enter the account login details that have WebDAV access rights to connect to the folder.
6. Enter a name for this network place.
7. The Web folder has been successfully created.
8. You can locate the web folder in the "Network Location" section in "Computer".
9. You can connect to the folder though this link via HTTP/WebDAV.

## Mac OS X

Follow these steps to connect to your QGW system via WebDAV on Mac OS X.

Client Operating System: Mac OS X Snow Leopard (10.6.1)

1. Open "Finder" > "Connect to Server", and enter the URL of the folder. Format:  
http://QGW\_IP\_or\_HOST\_NAME/SHARE\_FOLDER\_NAME
2. Enter the account login details that have WebDAV access rights to connect to the folder.
3. You can connect to the folder through this link via HTTP/WebDAV.
4. You can also find the mount point in the "SHARED" category in Finder and make it one of the login items.

These instructions are based on Mac OS X 10.6, and can be applied to 10.4 or later.

### Ubuntu

Follow these steps to connect to your QGW system via WebDAV on Ubuntu.

Client Operating System: Ubuntu 9.10 Desktop

1. Open "Places" > "Connect to Server..."
2. Select "WebDAV (HTTP)" or "Secure WebDAV (HTTPS)" for the Service type according to your QGW system settings and enter your host information. Enter the account login details that have WebDAV access rights to connect to the folder. Click "Connect" to initialize the connection.
3. The WebDAV connection has been successfully established, a linked folder will be automatically created on the desktop.

### MySQL Management

Install phpMyAdmin and save program files in the Web or Qweb share of the QGW series. You can change the folder name and connect to databases by entering the URL in the browser.

**Note:** The default username of MySQL is "root". The password is "admin". Change the root password **immediately** after logging in to the phpMyAdmin management interface.

### SQLite Management

Follow these steps or refer to the INSTALL file in the downloaded SQLiteManager-\*.tar.gz? to install SQLiteManager.

1. Unpack the downloaded file SQLiteManager-\*.tar.gz.
2. Upload the unpacked folder SQLiteManager-\* to \\QGW IP\Web\ or \\QGWIP\Qweb.
3. Open a web browser and go to http://QGW IP/SQLiteManager-\*/.?:
  - o The symbol "\*" refers to the version number of SQLiteManager.

## Virtual Host

A virtual host is a web server technique that provides the capability to host more than one domain (website) on one physical host and offers a cost-effective solution for personal and small businesses with such need. You can host up to 32 websites on the QGW series with this feature.

### Before you Start

In this tutorial we will use the information provided in the below table as a reference guide.

Host name	WAN/LAN IP and port	Document root	Demo web application
site1.mysite.com	WAN IP:	/Qweb/site1_mysite	Joomla!
site2.mysite.com	111.222.333.444	/Qweb/site2_mysite	WordPress
www.mysite2.com	LAN IP: 10.8.12.45 (QGW series) Port: 80 (QGW series)	/Qweb/www_mysite 2	phpBB3

Before starting, make sure you have checked the following items:

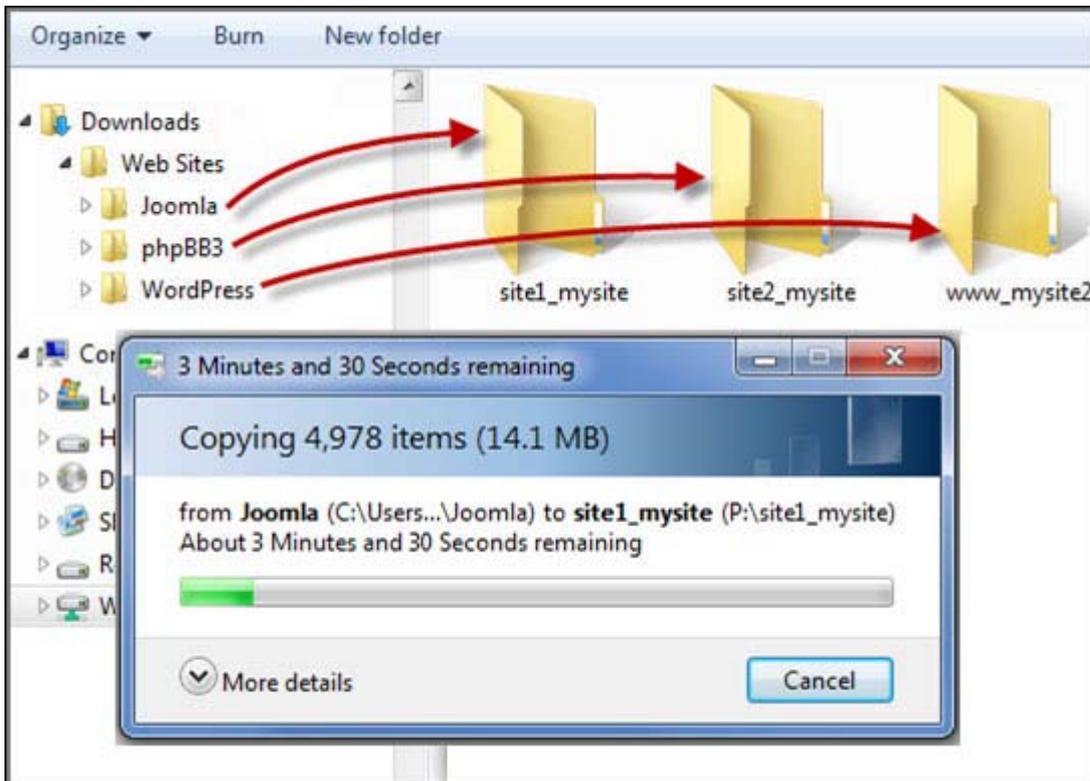
- Web Server: Enable Web Server in "Applications" > "Web Server".
- DNS records: The host name must point to the QGW series WAN IP. You can normally configure this from your DNS service providers.
- Port forwarding: If the web server listens on port 80 you need to configure port forwarding on your router to allow inbound traffic from port 80 to the LAN IP (10.8.12.45) of your QGW series.
- SSL certificate import: If you are going to enable SSL connection for the website and intend to use your own trusted SSL certificates you can import certificates from within the administration backend under "System Settings" > "Security" > "Certificate & Private Key".

### Using Virtual Host

Follow these steps to use virtual host:

1. Select "Enable Virtual Host" and click "Apply".
2. Click "Create a Virtual Host".
3. Enter the host name and specify the folder (under Web or Qweb) where the web files will be uploaded to.

- Specify the protocol (HTTP or HTTPS) for connection. If you select HTTPS, make sure the option "Enable Secure Connection (SSL)" in Web Server has been enabled.
- Specify the port number for connection.
- Click "Apply".
- Continue to enter the information for the rest of the sites you want to host on the QGW series.
- Create a folder for each website (site1\_mysite, site2\_mysite, and www\_mysite2) and start transferring the website files to the corresponding folders.



Once the files transfer is complete, point your web browser to the websites by [http://QGW\\_host\\_name](http://QGW_host_name) or [https://QGW\\_host\\_name](https://QGW_host_name) according to your settings. In this example, the URLs are:

- <http://site1.mysite.com>
- <http://site2.mysite.com>
- <http://www.mysite2.com>

Using the above example, you would see the Joomla!, phpBB3, and WordPress sites respectively.

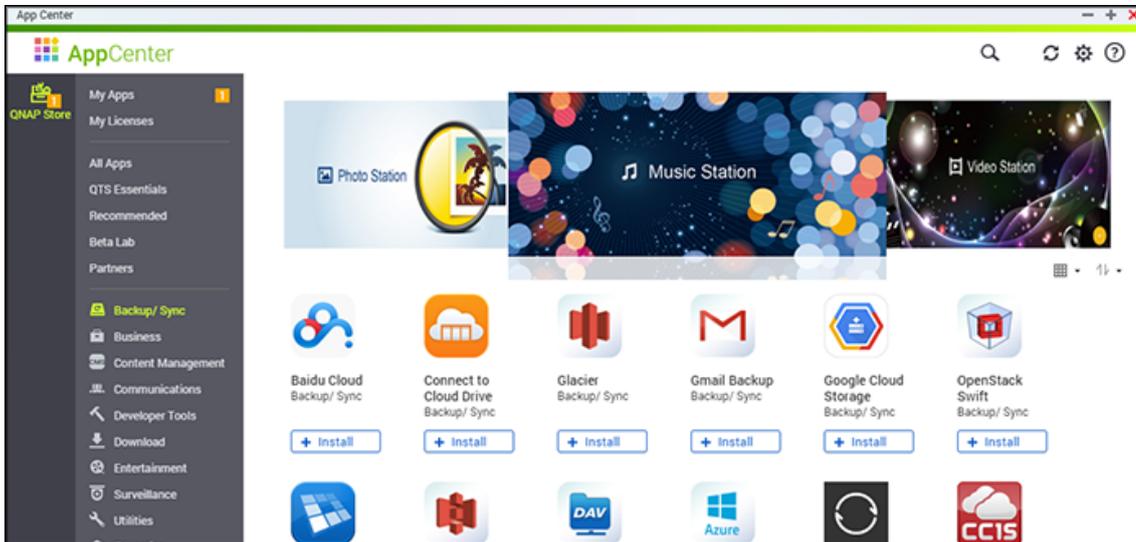
# Other Applications

Various applications are provided to enhance your user experiences. For details on these applications, refer to the following links:

- [App Center](#)
- [DLNA Media Server](#)
- [Download Station](#)
- [HybridDesk Station](#)
- [Multimedia Management](#)
- [myQNAPcloud Service](#)
- [Photo Station](#)
- [Station Manager](#)
- [Transcode Management](#)
- [Video Station](#)

# App Center

The App Center is a platform for the distribution of QGW system apps. Users can search for, install, remove and update apps developed by QNAP and third-party developers to expand services and add new features to the QGW series.

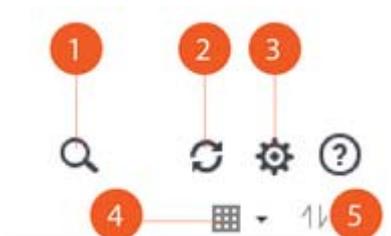


## Starting App Center

The App Center can be launched from the App Center shortcut on the Main Menu.

## Familiarizing yourself with App Center

### Menu Bar



No	Name	Description
1	Search	Search for Apps that are available to install on the QGW series.
2	Refresh	Refresh the current page.
3	Settings	<ul style="list-style-type: none"> <li>Install Manually: Browse to upload and manually install a QPKG add-on. You can also find information on App add-on developments</li> </ul>

		<p>here.</p> <ul style="list-style-type: none"> <li>• App Repository: If you have an URL provided by a third-party community or developer, you can add or modify it here to import applications from other sources.</li> <li>• QTS Gateway Help</li> </ul>
4	View Mode	Switch to item mode or list mode for the apps.
5	Sort	Sort apps by category, name, or release date, in an ascending or descending fashion.

**Left Panel**

- My Apps: List Apps that are currently installed on the QGW series.
- My Licenses: List licenses for all Apps to be installed on the QGW series. You can also add and activate your licenses.
- All Apps: List all Apps that can be installed on the QGW series.

**Using App Center**

**Searching apps**

To search for an App, enter the keyword in the search bar.

**Installing, updating and removing apps**

To install an app, click the "+ Install" button and the installation process will begin. After the installation process is complete, the "+ Install" button will turn to the "O Open" button and you can directly click this button to launch this newly installed app. This newly installed app will then show up in "My Apps".

**Note:**

- Make sure the QGW series is connected to the Internet.
- IEI is not responsible for troubleshooting any issues caused by open source software/add-ons. Users are encouraged to visit the QNAP community forum or contact the creators of the open source software for solutions.
- When installing an add-on that requires a prerequisite app, the prerequisite add-on will be automatically added to the installation queue prior to the dependent add-on.
- If the app update process is canceled before it is finished, please re-install the app from the App Center.

To update an App, click "Update" and click "OK" to confirm. Alternatively, you can click "Update All" on the menu bar to install all updates and "Refresh" to check for the latest updates. The button will turn to "Open" to signify that the update is complete. You can also click the down arrow icon on the

button to open an installed app, stop an app (the button will turn to "Start" after you stop an app and you can click it to start the app again), remove an app, or set to display the app on the administrator's main menu, every user's main menu, or the login screen as a shortcut.

**Note:** Click the on/off button in an App icon to enable or disable an App.

### **Offline Installation**

To install apps when the QGW series is offline or to install beta apps that are not officially available on the QNAP App Center, users can download the application (\*.qpkg) from the QNAP website (<http://www.qnap.com/go/qpkg.html>) or forum (<http://forum.qnap.com/>), unzip the files, and click "Install Manually" on the menu bar to install the Apps manually.

# DLNA Media Server

The QGW series supports two types of DLNA Media Servers: DLNA Media Server and Twonky Media DLNA Server.

Enable DLNA Media Server (Beta)

Service Name:

Select default user account:  ⓘ

**Note:**

DLNA Media Server requires [Media Library](#) to be enabled. Please configure the settings in "Applications" > "Multimedia Management" > "[Media Library](#)".

The displayed contents of DLNA server will be based on the system administrator account permissions and media library settings.

Enable TwonkyMedia DLNA Server

In order to start the service of TwonkyMedia, please install it from "[App Center](#)" first.

DLNA Media Server is developed by QNAP, and Twonky Media DLNA Server is a third-party media server. To allow DLNA media players to access and play the multimedia content via DLNA Media Server, enable the DLNA Media Server and configure the Media Library and the default user account.

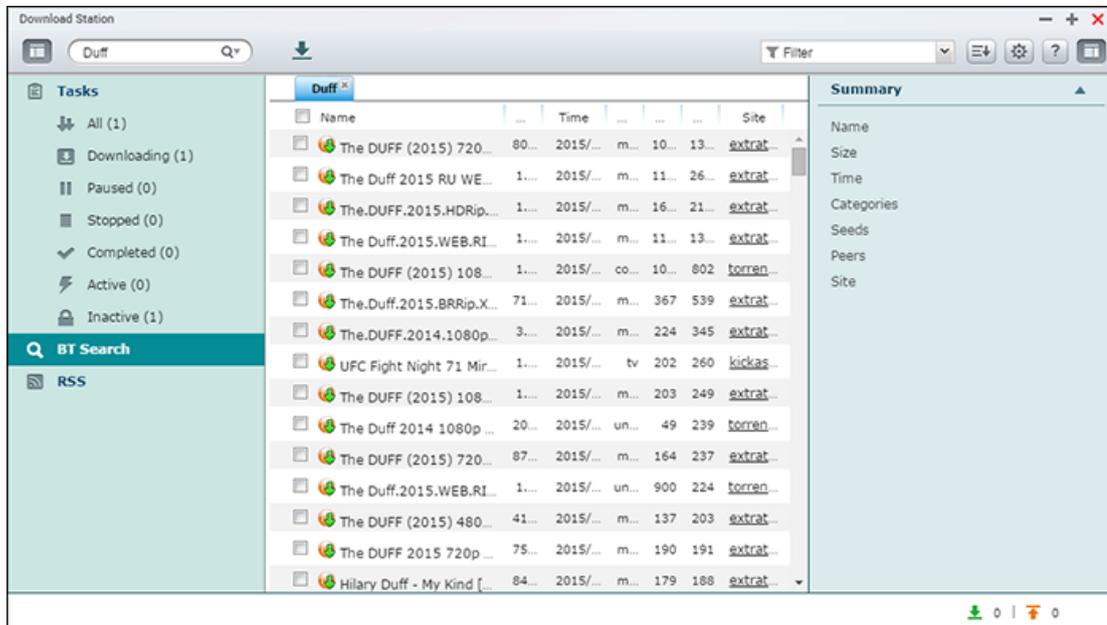
**Note:** The contents allowed to be browsed on devices connected to the media server are based on the shared folder permission set for the default user account. Viewers can only watch multimedia contents from the media folders that the default user account is assigned the permission with. For media folder setup, please refer to the chapter on Multimedia Management. For permission assignment, please refer to the chapter on [Shared Folder](#).

To allow DLNA players to access and play multimedia content via Twonky Media DLNA Server, enable it and click the link (<http://QGW IP:9000/>) to enter the TwonkyMedia DLNA Media Server configuration page. Go to "TwonkyMedia Settings" > "Basic Setup" to configure basic server settings. The Qmultimedia or Multimedia folder contents will be shared to digital media players by default. You can go to "Basic Setup" > "Sharing" > "Content Locations" to change the folder or add more folders. After configuring the settings, you can upload music, photos, and videos to these specified folders.

**Note:** If you upload multimedia files to the default folder but the files are not shown in the Media Player, click "Rescan content directories" or "Restart server" on the DLNA Media Server configuration page.

# Download Station

Download Station is a web-based download tool that allows you to download files from the Internet through BT, PT, Magnet Link, HTTP/HTTPS, FTP/FTPS, Xunlei, FlashGet, qqdl as well as Baidu Cloud downloads and subscribe to RSS feeds. With the BT Search function, you can easily find BT seeds to download and make your QGW series as 24/7 download center.



This chapter covers the following topics:

- [Starting Download Station](#)
- [Familiarizing yourself with Download Station](#)
- [Download Station Settings](#)
- [Using Download Station](#)

**Important:** The Download Station is provided for downloading authorized files **only**. Downloading or distributing unauthorized materials is against the law and may result in severe civil and criminal penalties. Users should be aware that they are subject to copyright restrictions and they will be held responsible for the consequences of their actions.

**Note:** For PT download, the supported client applications vary based on the PT sites. If the Download Station (libtorrent) is not in the client application list recommended by your PT sites, please search for an alternative one in the App Center.

## Starting Download Station

Depending on your QGW series model, Download Station may be enabled by default and can be launched from the Desktop or the Main Menu. If not, install and enable it in the App Center (for QTS Gateway 4.2 or later versions only.) Launch Download Station from the Main Menu/Desktop shortcut, or directly log into Download Station by going to:

[http://QGW\\_Name\\_or\\_IP/cgi-bin/Qdownload/qdownloadindex.cgi](http://QGW_Name_or_IP/cgi-bin/Qdownload/qdownloadindex.cgi)

## Familiarizing yourself with Download Station

### Menu Bar



No	Name	Description
1	Search Bar	Enter a keyword in the search bar, click the magnifier button to select the search engines and press enter to search for BT seeds. Please note that the BT search feature is only available after you agree to the terms and conditions in "Settings" button on the main menu > "BT" > "BT Search".
2	Add	Add a BT seed by entering the URL or upload a torrent file from the local PC.
3	Start	Start BT tasks.
4	Pause	Pause BT tasks
5	Stop	Stop BT tasks.
6	Remove	Remove BT tasks or remove BT tasks and their data
7	Action	Start all, pause all, or pause all download tasks for a specified time period, remove all completed tasks, remove all completed tasks and delete data.
8	Download	After you select BT seeds from the search result, click this button to download them.
9	Filter	Enter a keyword in the box or click the drop down list to select the categories and filter the searched BT seeds.
10	Sort	Sort tasks by dates that tasks are created or task types.

11	Settings	Configure BT or RSS settings (refer to the Download Station Settings section below.)
----	----------	--

### Left Panel

- **Tasks:** List all BT tasks based on their download status (All, Downloading, Paused, Completed, Active and Inactive.) Right click on a task to start it, pause, set priority and remove a BT task (and its data) and edit downloads.
- **BT Search:** List all BT seeds searched using the BT Search Bar. Right click a searched BT seed to download that seed (create a task), open the link URL, or download the torrent file.
- **RSS:** List, add, edit, delete or update RSS feeds.

### Download Station Settings

Click "Settings" to configure Download Station.

#### Global Settings

- **Download Schedule:** Select continuous download or specify the download schedule. When setting the download schedule, select "Full speed" to use the global speed limit (unlimited) for all the download tasks. Select "Limited" to apply the speed limit settings of the downloaded services.
- **Notification:** Select to send a notification by email when a download task completes (SMTP settings must be configured properly in "System Settings" > "Notification".)
- **Search:** Agree to enable the BT search function.

#### HTTP

- **Connection:** Specify the maximum number of concurrent HTTP downloads.
- **Bandwidth Limit:** Specify the maximum download rate of HTTP download tasks. 0 means unlimited (the maximum number of concurrent HTTP downloads is 30.)

#### FTP

- **Connection:** Specify the maximum number of concurrent FTP downloads.
- **Bandwidth Limit:** Specify the maximum download rate of FTP download tasks. 0 means unlimited (the maximum number of concurrent FTP downloads is 30.)

#### BT

- **Connection Setting:**
  - Specify the ports for BT download. The default port numbers are 6881-6889.
  - Enable UPnP port mapping: Enable automatic port mapping on the UPnP supported gateway.

- Enable DHT network: To allow the QGW series to download the files even no trackers of the torrent can be connected, enable DHT (Distributed Hash Table) network and specify the UDP port number for DHT.
- Protocol encryption: Enable this option for encrypted data transfer.
- Bandwidth Limit: Specify the maximum download rate of BT download tasks.
  - Global maximum concurrent downloads: Specify the maximum number of concurrent BT downloads (the maximum number of concurrent downloads is 30)
  - Global maximum upload rate (KB/s): Enter the maximum upload rate for BT download. 0 means unlimited.
  - Global maximum download rate (KB/s): Enter the maximum download rate for BT download. 0 means unlimited.
  - Maximum upload rate per torrent (KB/s): Enter the maximum upload rate per torrent. 0 means unlimited.
  - Global maximum number of connections: The maximum number of allowed connections to the torrent.
  - Maximum number of connected peers per torrent: The maximum number of allowed peers to connect to a torrent.
- Seeding Preferences: Specify the share ratio for seeding a torrent and the sharing time. The share ratio is calculated by dividing the amount of uploaded data by the amount of downloaded data.
- Proxy: specify the proxy server for BT download. Select the proxy type and enter the host IP and port, login username and password for the proxy server. For details on the setup of the proxy server, please refer to its user manual.
- BT Search: Select the BT engines to enable for BT search on the Download Station.

## RSS

Update: Enable RSS download and specify the time interval for the QGW series to update the RSS feeds and check if any new contents that match the filters are available.

## Add-on

You can enable and disable supported BT sites, torrent search engines and indexers on this page. New BT sites, search engines and indexers can be added as an Add-on to enrich the possibilities of Download Station.

**Tip:** You can click the following link to download the developer guide for creating Download Station Add-ons: [http://download.qnap.com/dev/download-station-addon-developers-guide\\_v4.pdf](http://download.qnap.com/dev/download-station-addon-developers-guide_v4.pdf)

## File Hosting Account

You can save the login information for up to 64 HTTP and FTP accounts. To add login information, click "Add Account". Enter the host name or IP, username and password. To allow the login information to appear for account selection when configuring HTTP or FTP download, select "Enabled" next to the newly added account. To edit the settings of an account, select an entry on the list and click "Edit Account". To delete an account, select an entry on the list and click "Delete Account".

## Using Download Station

### Adding download task(s)

There are three ways to add download tasks:

1. Drag and drop BT/PT files from the local PC to Download Station or click "+" button to add BT/PT files or multiple URLs (HTTP/FTP/Magnet link.)
2. You can search for BT files using the BT search function to add download tasks.
3. In "RSS" on the left panel, you can add RSS feeds. Download Station will load all feeds from RSS for you to download.
4. Designate a location on the QGW series for the in-progress files and completed downloads.

#### Note:

- The maximum number of concurrent downloads for is 60 (30 BT/PT and 30 HTTP/FTP).
- Dragging & dropping BT files from PC to Download Station is only supported by Chrome and Firefox.

### Adding HTTP, FTP, Magnet download tasks

To add an HTTP, FTP, or Magnet download task, click "Start" on the Menu Bar. Enter the URL of the download task (one entry per line.) Then select the download type: HTTP/FTP, or Magnet Link. Designate a location on the QGW series for the in-progress files and completed downloads. If a username and password is required to access the file, select "Use credentials" and select a pre-configured account (Settings > Account List) or enter a username and password. Then click "OK". The QGW series will download the files automatically.

**Note:** You can enter up to 30 entries at one time.

### Managing downloads in a BT seed

You can right click on a task and select "Edit Downloads" to only select the files within a BT seed that you want to download.

### **Limiting the download/upload speed**

To limit the bandwidth usage of the Download Station, configure the settings in "Settings" > "HTTP", "FTP", or "BT" > "Bandwidth Limit".

### **Scheduling downloads**

To set download schedules, go to "Settings" > "Global" > "Download Schedule". After enabling the download schedule, select "Full speed", "Turn off", or "Limited" and then click the preferred time slots.

### **Sending a notification after a download task is complete**

Go to "Settings" > "Global"> "Notification" and enable "Email".

### **Subscribing to and managing RSS feeds**

You can subscribe to RSS feeds using the Download Station and download the torrent files in the feeds:

1. Click "+" next to "RSS" on the left panel to add an RSS feed.
2. Enter the URL and the label.
3. To download a torrent file from an RSS feed, select the file and click the down arrow button or right click the feed and select "Download".
4. The QGW series will automatically download the file. You can view the download status in the Downloading list.

To manage the RSS subscriptions, right click on an RSS feed label. You can open the RSS Download Manager, add, update, edit, or delete an RSS feed.

### **Downloading torrent files using RSS Download Manager**

You can use the RSS Download Manager to create and manage filters to download particular torrent files for BT Download.

- To add a filter, first launch the RSS Download Manager, select a label and click "Add".
- Enter the filter name and specify keywords to include and exclude.
- Select the RSS feed to apply the filter settings.
- You may also specify the quality of the video torrent files (leave it as "All" if you do not need this function or the torrent file is not a video.)
- Episode number: Select this option to specify particular episodes or a series of episodes. For example, to download episodes 1-26 of season 1 of a TV program, enter 1x1-26. To only download episode 1 of season 1, enter 1x1.
- Select the time interval for automatic update of RSS feeds. The QGW series will update the RSS feeds and check if any new contents that match the filters are available.
- Click "Apply" to save the filter or "Cancel" to cancel or exit.
- To delete a filter, select the filter from the list and click "Delete".

### Shortening BT seeding time

Go to "Settings" > "BT" > "Bandwidth Limit">"Seeding Preferences".

Change the "Share Ratio" to a smaller percentage or modify "Share Time" to shorten BT seeding time.

### Sharing by multiple users

Administrators can grant Download Station access to QGW system users. Follow these steps to grant access to QGW system users:

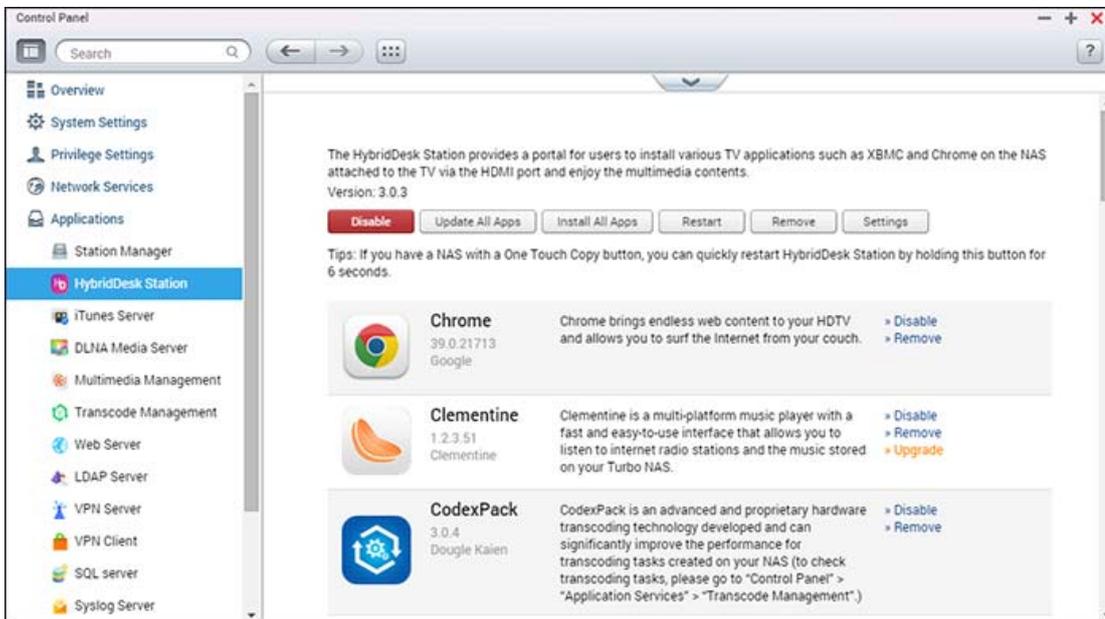
1. Go to "Control Panel" > "Privilege Settings" > "Users"
2. Click the "Edit Application Privilege" button under "Action" for the user
3. Grant permission for Download Station > "Apply".

#### **Tip on slow BT download rates or download errors:**

1. The torrent file has expired, the peers have stopped sharing this file, or there is error in the file.
2. The QGW series has been configured to use a fixed IP but the DNS server is not configured or it has failed.
3. Set the maximum number of simultaneous downloads as 3-5 for the best download rate.
4. The QGW series is located behind a NAT router. The port settings have led to slow BT download rate or no response. You can try the following means to solve the problem:
  - a. Manually open the BT port range on NAT router. Forward these ports to the LAN IP of the QGW series.
  - b. Recent QGW series firmware supports UPnP NAT port forwarding. If your NAT router supports UPnP, enable this function on the NAT. Then enable UPnP NAT port forwarding of the QGW series. The BT download rate should be enhanced.

# HybridDesk Station

HybridDesk Station is a platform where numerous home and office apps can be installed to enhance your entertainment and productivity needs.



This chapter covers the following topics:

- [Setting up HybridDesk Station](#)
- [Using HybridDesk Station](#)
- [Importing Media Contents to your QGW Series](#)
- [Configuring HybridDesk Station](#)

## Setting up HybridDesk Station

Create your lovely media environment by following these steps:

1. **Setting up the environment of the HybridDesk Station: Connect the QGW series to the HDMI TV with a HDMI cable**
  - There are two different ways to control the HybridDesk Station.
    - USB keyboard or mouse
    - Qremote: remote app, designed exclusively for the HybridDesk Station.

**Note:** If you want to use Chrome, you must use the Qremote mouse function or use a USB mouse that is connected to the QGW series.

## 2. Installing the HybridDesk Station

- Go to "Applications" > "HybridDesk Station" and click the "Get Started Now" button. The system will automatically install the HybridDesk Station.

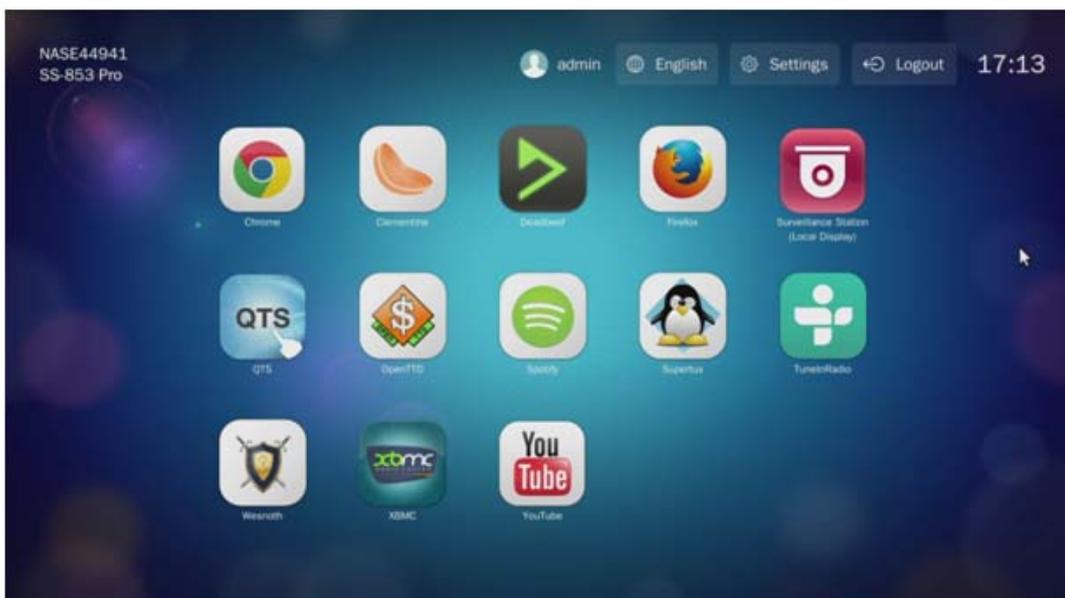
## 3. Choosing the applications to install

- HybridDesk Station: The HybridDesk Station portal, which allows you to use the following applications on the TV screen.
- My NAS: Enter the local NAS administration web page to view the functions and settings.
- Surveillance Station (Local Display): An application that allows QGW devices to output high-resolution video from IP cameras.

### Note:

- Using Kodi, Chrome, or other applications may affect the hard drive hibernation of the QGW series. Remember to exit the application and return to the HybridDesk Station portal.
- For the best HybridDesk Station experience, we recommend using a QGW series with at least 2GB memory.
- To use the AirPlay function provided by Kodi, we recommend using a QGW series with at least 2GB memory.
- The HybridDesk Station will restart when formatting an USB external device.
- The first time Kodi is launched, it will index the "Multimedia" shared folder and it may consume a lot of system resources if the folder contains a lot of multimedia files.

After installation, choose your preferred language on the TV screen. Then, you will see the HybridDesk Station portal as shown here.



4. **Enjoying the HybridDesk Station: At the HybridDesk Station portal, simply choose the application you want to use to start the service.**

Play photos directly on your TV by XBMC or other applications.

## **Using HybridDesk Station**

### **Taking Pictures with Smart Phone and Watching them on TV**

The first part is done by Qfile on your phone:

1. Use Qfile to browse your QGW series.
2. Choose the multimedia shared folder.
3. Select the upload function.
4. Take a picture and upload it to the QGW series.

The second part is performed by the HybridDesk Station on your TV:

5. Turn on your TV and choose Kodi.
6. Choose "Pictures".
7. Select the "Multimedia" folder.
8. Double click the picture you just uploaded.

### **Viewing Photos on your USB Device or Camera**

Steps:

1. Connect a USB device or camera to the QGW series.
2. Choose "Pictures".
3. Choose "USBDisk".
4. Select the photo you want to view.

### **Importing Media Contents to your QGW series**

Use one of the several types of network protocols (Samba, AFP, FTP, and NFS) to save the media content files in the "Multimedia" or "Qmultimedia" shared folder, or copy them from an external USB device.

To browse media contents of different folders than the default "Multimedia" shared folder, perform the following steps:

1. Choose "Files" under "Videos".
2. Choose "Add Videos".
3. Click "Browse".
4. Choose "Root filesystem".
5. Choose "share".

6. For example, if you want to add the "Download" shared folder, choose "Download".  
Otherwise, just choose the shared folder you would like to add as a video source.
7. Click "OK" to add this source.
8. You will see the "Download" shared folder in the list.

**Note:**

- If you encounter any video playback quality issues with some video formats, you can enable the following settings on Kodi: Go to "Setting" > "Video" > "Playback", and then enable "Adjust display refresh rate to match video" and "Sync playback to display".
- Depending on the data type, some files may not be playable.

### Chrome

Select the Chrome application at the main page of HybridDesk Station. You can surf the web like using a web browser on your PC.

**Note:** If you want to use Chrome, you must use the Qremote mouse function or use a USB mouse that is connected to the QGW series.

### Surveillance Station (Local Display)

Monitor IP cameras and playback recordings stored on the QGW series.

### YouTube

Enjoy videos on YouTube via HybridDesk Station.

### MyNAS

Enter the local NAS administration web page to view the NAS functions and settings.

### Configuring HybridDesk Station

Configure the HybridDesk Station by choosing "Settings" at the HybridDesk Station portal and HybridDesk Station in QTS Gateway.

- HybridDesk Station portal:
  - App: Applications can be enabled or disabled here.
  - Display: Change the screen resolution and set up to turn off the screen after an amount of idle time.
  - Preferences: Here you may change the language or type of remote control and audio output. The default setting is HDMI. If there is an installed USB sound card, you can choose that option in the Audio Output.
- HybridDesk Station in QTS Gateway:

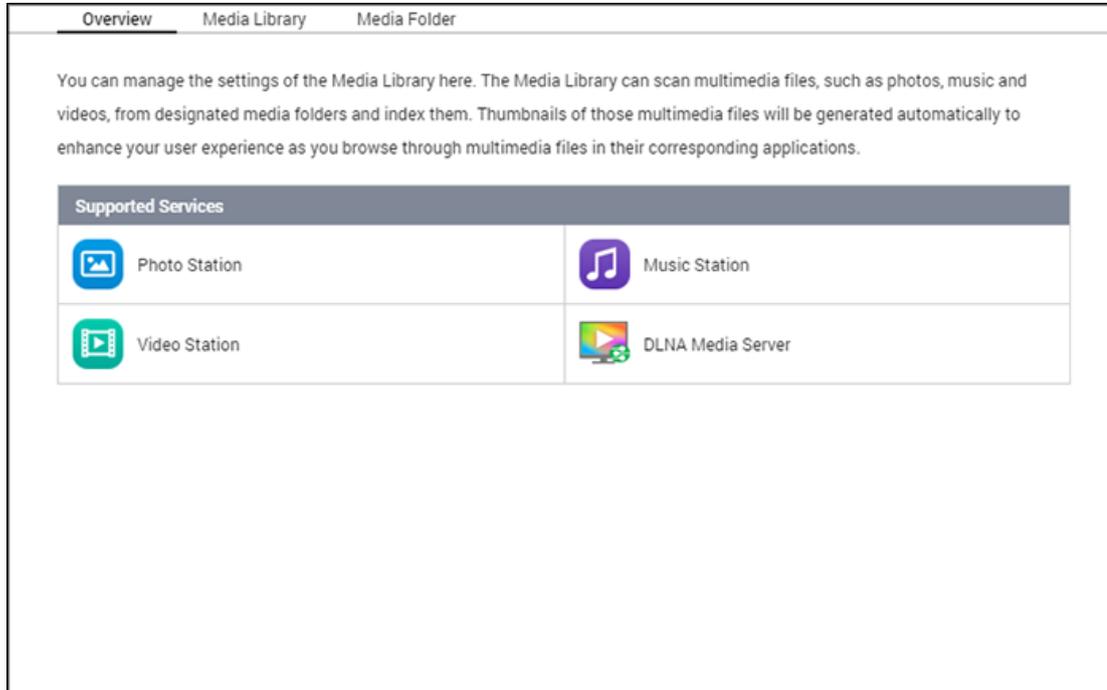
- Output resolution: Change the resolution for the HybridDesk Station portal screen. Before you change this setting, please make sure that no apps are opened in the HybridDesk Station portal.
- Overscan: This setting can reduce the visible area of a video displayed on the HybridDesk Station portal. The higher the percentage, the more the visible area will be reduced.

**Additional Reference:**

[How to use Surveillance Station \(Local Display\) in HD Station.](#)

# Multimedia Management

The Media Library service scans for photos, music, and videos from designated media folders and indexes them for usage in multimedia applications. Thumbnails for the media files will be automatically generated to enhance your user experience as you browse through them in their corresponding applications.



## Media Library

- Scan Setting: Three options are provided for the media scan:
  - Real-time scan: New files are scanned in as soon as they are added to media folders.
  - Scan by schedule: Specify a start and end time for the scan, and it will be automatically conducted on a daily basis.
  - Manual Scan: You must click "Scan now" to check for new media.
- Set media scanning priority to high: The option will allow the media library to immediately process media files in order to quickly generate thumbnails. When the QGW series needs to run scan tasks and transfer files at the same time, it will lower the file transfer speed and prioritize media scan tasks.
- Multimedia code page setting: Change this setting to the corresponding code for non-UTF media files for fonts and characters in the associated applications to be displayed correctly.
- Rebuild media library indexing: By rebuilding the media library, the QGW series will scan the specified media folders and replace the existing library with a new one.

The media library is enabled by default. In some cases, the media library needs to be disabled (when multimedia applications are not installed on the QGW series.) To disable the media library, click "Deactivate Media Library". If the media library is not enabled, services like Photo Station, Video Station, and as well as the DLNA Media Server will not function correctly. To re-enable the media library, click "Activate Media Library".

**Note:**

- If the media library is disabled, services like Photo Station and the DLNA Media Server will not function correctly.
- Image files with a width or height less than 400 pixels will not be indexed and will not have any thumbnails generated.

## **Media Folder**

Media folders are shared folders on the QGW series that are scanned for multimedia files.

"/Multimedia" and "/Home" are the default media folders on the QGW series (from QTS Gateway 4.2, all default shared folders on the QGW series are identified as media folders for the purpose of multimedia application services.) To add media folders: click "Add", select media types and folders from the list, and click "Add". To change scanned file types for the media folders, first uncheck the media file types and click "Apply". To remove media folders, first select media folders from the list, and then click "Delete" and "Apply".

# myQNAPcloud Service

myQNAPcloud provides host name registration, mapping of a dynamic QGW system IP to a domain name, and auto port mapping for UPnP routers on the local network. Use the myQNAPcloud wizard to register a unique host name for the QGW series, configure automatic port forwarding on the UPnP router, and publish services for remote access over the Internet.



To use the myQNAPcloud service, make sure the QGW series has been connected to an UPnP router and the Internet and click the myQNAPcloud shortcut from the QGW Series Desktop or Main Menu.

This chapter includes two parts. The first part deals with the myQNAPcloud App you use on the QGW series and covers the following setup:

- [myQNAPcloud Wizard](#)
- [Auto Router Configuration](#)
- [My DDNS](#)
- [Cloud Portal](#)
- [CloudLink](#)
- [Access Control](#)
- [SSL Certificate](#)

The second part of the chapter focuses on the following topic:

- [myQNAPcloud Portal](#) (a portal for remote accessing and managing multiple QGW systems across the Internet.)

## myQNAPcloud Wizard

It is recommended to use the wizard the first time you use myQNAPcloud. Follow these steps:

1. Click "Get Started" to use the wizard.
2. Click "Start".
3. Fill out your myQNAPcloud ID(QID) and password. Click "Next" (or click "Create myQNAPcloud account" to sign up a myQNAPcloud account if you don't already have an account.)
4. Enter a name to register your QGW series and click "Next".
5. Select to enable the myQNAPcloud services (Auto Router Configuration, DDNS, Publish Services and CloudLink) and set the level of access control. Click "Next".
6. The wizard will configure your router automatically.
7. Review the summary page and click "Finish" to complete the wizard.

## Auto Router Configuration

In "Auto Router Configuration", you can enable/disable UPnP port forwarding. When enabled, your QGW series is accessible from the Internet via the UPnP router.

**Note:** If there is more than one router on the network, only the one which is set as the default gateway of the QGW series will be detected.

If no UPnP router is found on the local network, click "Rescan" and "Diagnostics" to check the diagnostic logs. If the UPnP router is incompatible with the QGW series, click the tooltip icon (!) and then click "UPnP Router Compatibility Feedback..."

([http://www.qnap.com/go/compatibility\\_router.html](http://www.qnap.com/go/compatibility_router.html)) to contact technical support. Select the services to be allowed for remote access and click "Apply to Router". The QGW series will automatically configure the port forwarding on the UPnP router. You will then be able to access services from the Internet.

### Note:

- If more than two QGW systems are connected to one UPnP router, please specify a different port for each QGW system. If the router does not support UPnP, users must manually configure port forwarding on the router. Please refer to these links:
- Application notes: <http://www.qnap.com/go/notes.html>
- FAQ: <http://www.qnap.com/faq>
- UPnP router compatibility list: [http://www.qnap.com/UPnP\\_Router\\_Compatibility\\_List](http://www.qnap.com/UPnP_Router_Compatibility_List)

## My DDNS

By enabling the myQNAPcloud DDNS service, you can connect to the network services on your QGW systems by using your specified internet address. To change your myQNAPcloud

DDNS domain name, click the "here" link on the page. Your recent DDNS information will be shown here and you can click the "Update" button to refresh the result.

## Cloud Portal

With the Cloud Portal, web-based services (including File Station, Web Server, Photo Station, Secure File Station, Secure Web Server and Secure Photo Station) can be published to <http://www.myqnapcloud.com>. By enabling the services here, they will be opened for remote access even if they are not published. Enable the myQNAPcloud DDNS service and the QGW systems will automatically notify the myQNAPcloud server if the WAN IP address of the QGW systems has changed. To use the myQNAPcloud service, make sure the QGW systems has been connected to a UPnP router and the Internet.

### Note:

- The myQNAPcloud name of each QGW system is unique. One myQNAPcloud name can only be used for one QGW system.
- A registered myQNAPcloud name will expire in 120 days if your QGW system remains offline within that period. Once the name is expired, it will be released for registration by other users.
- For My DDNS, if the default port is not used, you will need to specify the port number when accessing network services.

1. In "Cloud Portal", web-based services are shown. Select "Publish" to publish the services to the myQNAPcloud website. Select "Private" to hide published services from public access. The private services on the myQNAPcloud website are only visible to specified users with the myQNAPcloud access code. If a disabled service is published, the service will be inaccessible even if the corresponding icon is shown on the myQNAPcloud website (<http://www.myQNAPcloud.com>.)
2. Set myQNAPcloud Access Code: Enter a 6-16 characters (a-z, A-Z, 0-9 only) code that QGW system users will need to enter when they attempt to view private services on the myQNAPcloud website.
3. Click "Add Users" and specify up to 9 local QGW system users who are allowed to view private services published on the myQNAPcloud website.
4. Select the connection method: the myQNAPcloud Connect (VPN) utility and/or myQNAPcloud website.
5. To send instructions to use the myQNAPcloud service to users via email, select the users and click "Send Invitation".
6. Enter the email address. Click "Send".

**Note:** To use this function, the email server settings must be properly configured in "System Settings" > "Notification" > "SMTP Server".

## CloudLink

CloudLink is an innovative service for remote access to your QGW series over the network without changing router settings - even if UPnP is not supported. After you enable the service (click the switch on the blue banner to enable/disable the service) the direct access link will be shown on the page and you can provide this link to your friends for them to access to your QGW series, using their mobile device or computer.

## Access Control

This function allows you to control who can search for your device and access published services on the myQNAPcloud website or with mobile apps remotely via CloudLink. The following options are available:

- **Public:** Everyone can search for your device on the myQNAPcloud website and access your public services.
- **Private:** Only you can access your QGW system remotely on the myQNAPcloud website or with mobile apps via CloudLink.
- **Customized:** You can specify who is allowed to access your device on the myQNAPcloud website or with mobile apps by entering their registered accounts here. Or you can add email addresses of your friends who are not currently myQNAPcloud members to send them an invitation. To set access controls, first set the "Device access controls" to "Customized", then click "Add" to add QID account holders.

## SSL Certificate

myQNAPcloud SSL certificates are used to provide secured connections between the QGW series and web browsers, providing authorization and connection encryption. Encrypted connections secure data and transactions. Before installing a myQNAPcloud certificate, an error may occur when you try to connect to your QGW series using HTTPS (for example: <https://nossll.myqnapcloud.com>.) The data transmitted in the connection is not protected against security threats. Unauthorized users have the potential to intercept data being sent between a QGW system and web browser.

Purchasing and installing a myQNAPcloud SSL certificate will bring you better protection when connecting your QGW series via DDNS.

**Note:** A myQNAPcloud SSL certificate can only be used on QGW series with QTS Gateway 4.2 or above.

### **Purchasing myQNAPcloud SSL certificates**

1. Sign into the myQNAPcloud website with your myQNAPcloud account and go to "SSL Certificate" on the left side.
2. Read and agree to the terms and conditions.
3. Choose the number of certificates you want to buy (only one certificate can be used on one device at a time) and complete the purchase and checkout process.
4. Confirm the order and return to the "SSL Certificate" page on the myQNAPcloud website.

### **Installing myQNAPcloud SSL certificates**

1. Log into your QGW series as an administrator and launch myQNAPcloud.
2. Select "SSL Certificate" on the left panel > click "Download and install" to install the certificate.
3. Choose one of your purchased certificates from the list > click "Confirm".

To install the same certificate on another device, log into the QGW series as an administrator, go to myQNAPcloud > "SSL Certificate" and click "Release" to release the certificate. Then, follow the same above steps to install that released myQNAPcloud SSL certificate on another device.

On the myQNAPcloud portal site, you can review the transaction history in "SSL Certificate" > "Transaction record". There are three transaction types:

- Apply: The certificate has been installed.
- Release: The certificate has been released from the device.
- Reissue: The certificated has been reissued due to a DDNS name change.
- Extend: The certificate's validity has been extended.

The system will remind you of the expiration date within 30 days of expiration. Please renew your certificate before it expires. To extend your certificate, log into the myQNAPcloud website and go to "SSL Certificate" > "Certificate License".

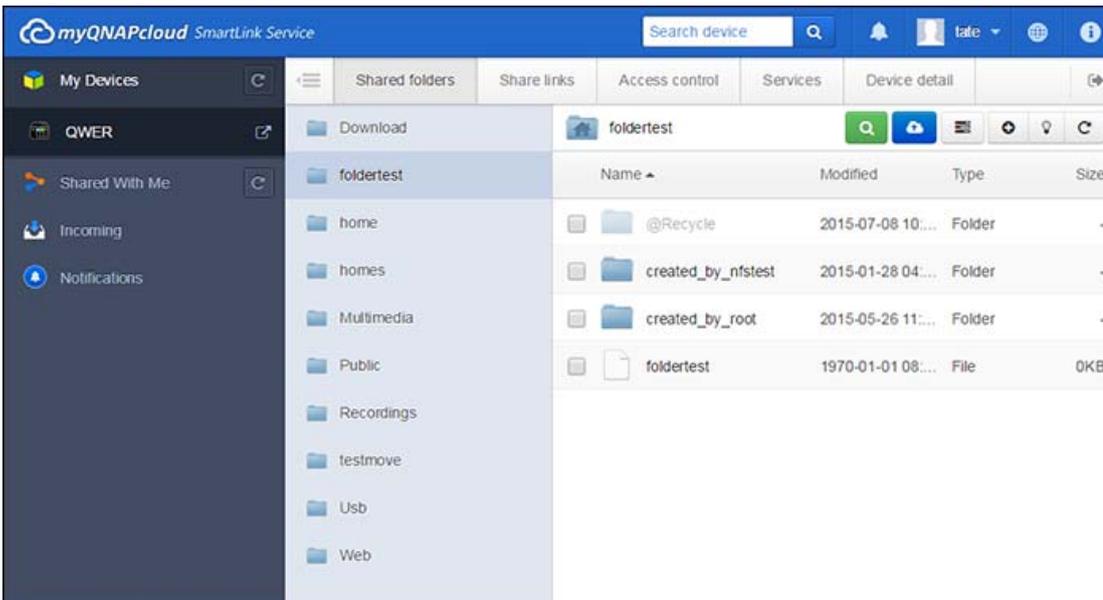
### **Note:**

- A myQNAPcloud SSL certificate can only be used on a QGW system with QTS Gateway 4.2 or above.
- To use this service, first download and install the myQNAPcloud SSL Certificate QPKG from the App Center.

## myQNAPcloud Portal

The myQNAPcloud portal ([www.myqnapcloud.com](http://www.myqnapcloud.com)) is an integrated web interface that allows you to:

- Manage and configure your myQNAPcloud account
- Access QGW system
- Use published services from other QGW system
- Open links shared with you
- Be notified of myQNAPcloud activities



You must configure your myQNAPcloud account using the myQNAPcloud App before logging into the myQNAPcloud portal.

### Managing and Configuring your myQNAPcloud Account

After launching myQNAPcloud or logging into your account on the myQNAPcloud website, click on your nickname (next to the notification icon in the top-right corner) > "User Profile".

On this page, you can:

- Update your profile
- Change your myQNAPcloud login password
- Add or edit your contact list
- Check application logs
- Monitor myQNAPcloud activities

### Accessing QGW System via myQNAPcloud Website

After you log into the myQNAPcloud web portal, you will see a list of QGW systems under "My Devices" on the left of the screen. Click on any of the QGW system and there will be a list of available actions to perform and you will be able to:

- Perform basic file management tasks as in File Station

- Manage share links
- Configure access controls (check the above [Access Control](#) section for more details)
- View and access published and private services (for private services, check the above [Cloud Portal](#) section for more details)
- Review and refresh device details or unregister the device

**Note:**

- Once you unregister your device from myQNAPcloud, all of the services will be stopped.
- You must install the CloudLink QPKG in the App Center before performing basic file management tasks or managing share links on the myQNAPcloud portal site.

### **Using published Services from other NAS Servers via myQNAPcloud Website**

The "Shared with me" feature allows you to quickly find your friend's devices and access their published services. Follow these steps to add a device and access its published services:

1. Log into the myQNAPcloud web portal
2. Type the device name of your friend's device in the search box in top right corner.
3. Click the "Add to Shared With Me" button (the gray heart icon)
4. Click "Shared With Me" to the left of the screen.
5. Click the newly added device from the list and the service you want to access.
6. Choose an access method.

### **Sharing Files and Opening Links Shared with You via myQNAPcloud Website**

If you share data to your friends who have registered on myQNAPcloud, they will see these shared links here.

To share a file on the myQNAPcloud portal site, follow these steps:

1. Log into the site
2. Select a device under "My Devices" on the left panel
3. Log into your device
4. Choose the folders or files you want to share
5. Click "Share" and fill out the required fields for the link (link name, domain name/IP, expiration, and password protection) > "Next" > and finish link recipient and email details > "Share".

To open a such link, first log into the myQNAPcloud website and click "Incoming" to the left of the screen and you will see the links you can click to access them.

**Note:** Before you use this feature, you must install the CloudLink QPKG in the App Center.

### **Be notified for myQNAPcloud activities**

The portal will notify you of myQNAPcloud activities. Examples of such activities are:

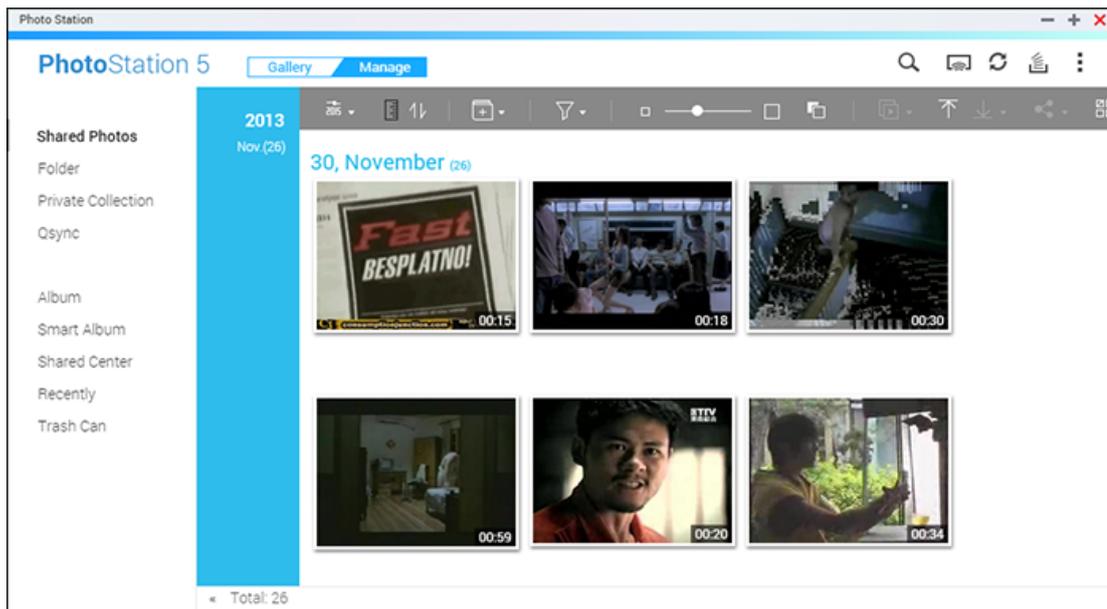
- Your friends have added your device as a favorite
- Your friends have created a shared link for you.
- Your friends have shared their device with you.

To check myQNAPcloud activities, follow these steps:

1. Log into the myQNAPcloud portal site
2. Click "Notifications" on the left of the screen (or the notification icon next to the device search box.)

# Photo Station

Photo Station (5.0) is an online photo album used to organize photos and videos on the QGW series and to share them with others across the Internet. With Photo Station, users can drag & drop photos into virtual albums, sparing them from having to tediously move/copy files around and helping to save storage space as they only need one copy of their photos on the QGW series when they create albums with special themes. Smart albums can also be used to automatically collect content that matches search criteria and helps users to neatly manage their photos.



This chapter covers the following topics:

- [Starting Photo Station](#)
- [Familiarizing yourself with Photo Station](#)
- [Using Photo Station](#)
- [Media Library and Privacy Settings](#)

## Starting Photo Station

Depending on your QGW series model, Photo Station may be enabled by default and can be launched from the Desktop or the Main Menu. If not, install and enable it in the App Center (for QTS Gateway 4.2 or later versions only) and follow these steps:

1. Import photos and videos to a shared folder on the QGW series. There are three ways to upload photos and videos to the QGW series: 1) Install Qfinder Pro on your PC or Mac, set up a network drive and upload files to your preferred shared folders. For details on setting up a network drive, check the [Connecting to Shared Folders](#) chapter; 2) Click "Shared Photos" or "Private Collection" in the left panel in Manage mode and click "Import" on the main menu to import photos or videos from the local PC. A new shared folder named with the date that files are uploaded will be created on the QGW series to store your uploaded files (for "Shared Photos", this newly-created shared folder is located under the "Multimedia" folder; for "Private Collection", this shared folder is located under the "/home" folder.) A corresponding album will be created under "Album" as well; and 3) Switch to the folder view browsing mode and drag & drop photos and videos to a preferred folder. Note that when using the first and third approach, you can choose the QGW folder to upload photos and videos into.

The Photo Station supports the following file formats:

Image	BMP, JPG, JPE, PNG, TGA, GIF, and more.
Video	API, MP4, and more.

**Tips on file upload:**

- The maximum size of an image file is 2GB.
- The maximum size of multiple files that can be uploaded at a time is 2GB.

2. Launch Photo Station from the Main Menu/Desktop shortcut, or directly log into Photo Station by going to: [http://QGW\\_Name\\_or\\_IP/photo/](http://QGW_Name_or_IP/photo/)

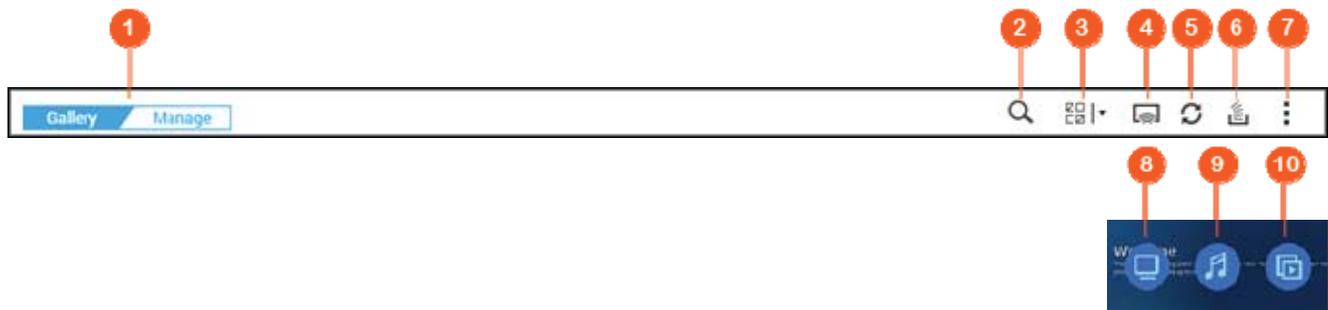
**Note:** The admin login credentials of Photo Station is the same as that of the QGW system administrator.

## Familiarizing yourself with Photo Station

In Photo Station, there are two modes that you can use: Gallery mode and Manage mode. Gallery mode is designed for a greater viewing experience, while Manage mode is provided for easier photo and video management.

## Gallery Mode

### Menu Bar



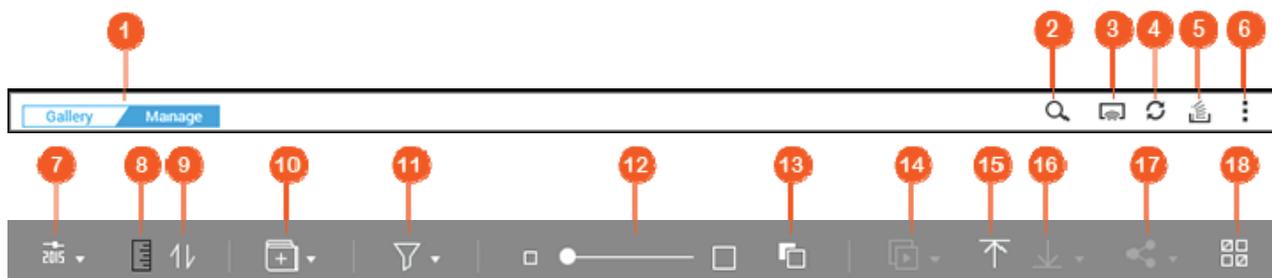
No	Name	Description
1	Gallery/Manage	Switch between Gallery mode and Manage mode.
2	Advanced Search Bar	Search for photos and videos by title, date taken, file size, resolution, camera brand, color label, rating, description or tag.
3	Multi-Select	Select multiple items at the same time.
4	Network Media Player	Locate compatible devices in different rooms over your home network.
5	Refresh	Refresh the current page.
6	Background Task	Show Photo Station tasks (such as uploading photos/videos to your QGW series or Picasa, Flickr, Weibo, or YouTube) that are currently running in the background.
7	Settings	Launch Quick Start and show the Photo Station online help.
8	Display	Switch between thumbnail and wallpaper display styles and configure display settings (including the gallery view, source, content filter, or sort) by moving your mouse over the button and click "Display Settings". Refer to the <a href="#">Viewing photos and videos</a> section for more details.
9	Music	Play/Pause background music. You can also choose the music source by moving your mouse over the button and clicking "Music Settings".
10	Slideshow	Play all of the photos in an album as a slideshow. You can also configure slideshow settings (including the speed, effect and music) by moving your mouse over the button and clicking "Slideshow Settings".

**Note:**

- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW series does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, please refer to the [Transcode Management](#) chapter.
- If your QGW series supports transcoding, please install the CodexPack App before using this function. The QGW series will try to transcode to a suitable format for your device. If your QGW series does not support transcoding, the QGW series will only output the original file format and the seek function may not work properly. In this case, please make sure that your device is compatible with the file format used by the video.
- Some video formats may experience issues when streaming via DLNA, Apple TV or Chromecast. If any of these issues arise during video playback, you can consider transcoding your videos into universally-compatible media formats. For more details on transcoding, please refer to the [Transcode Management](#) chapter.
- Some media players do not support pausing during playback. If this happens, playback will continue even if you use the pause feature.

**Manage Mode**

**Menu Bar**



No	Name	Description
1	Gallery/Manage	Switch between Gallery mode or Manage mode.
2	Advanced Search Bar	Search for photos and videos by title, date taken, file size, resolution, camera brand, color label, rating, description or tag.
3	Network Media Player	Locate compatible devices in different rooms over your home network.
4	Refresh	Refresh the current page.

5	Background Task	Show, pause, or cancel Photo Station tasks (such as uploading photos or videos to your QGW series or Picasa, Flickr, Weibo, or YouTube) that are currently running in the background.
6	Settings	<p>Configure Photo Station settings, launch the Quick Start, or show the Photo Station online help. There are four settings:</p> <ul style="list-style-type: none"> <li>• Content Filter: Select shared folders as the content source of the Photo Station. To add new shared folders as the content source, go to "<a href="#">Multimedia Management</a>".</li> <li>• Social Network Binding: bind with social networks for your friends to log into the Photo Station and browse shared albums.</li> <li>• Backup/Restore: Export or import a configuration file of all albums and smart albums for their configuration backup and restoration.</li> <li>• Miscellaneous: <ul style="list-style-type: none"> <li>○ Always ask me to enter my password when accessing Private Collection: Photo Station will prompt users for a password every time they try to access the Private Collection.</li> <li>○ Select a shared folder as the default folder to store photos uploaded to Shared Photos: Set a default shared folder to store uploaded photos.</li> <li>○ Automatically create matching album: An album with the same name you specified in the file upload process will be automatically created under "Album" on the left panel after you upload photos. If this is disabled, only the physical folder will be created under your designated upload shared folder.</li> <li>○ Always start in Manage mode: Check this option to always start Photo Station in Manage mode.</li> <li>○ Display Settings: Set the aspect ratio for video and image thumbnails.</li> </ul> </li> </ul>
7	Browsing Mode	Switch between different browsing modes (thumbnail browsing mode, list browsing mode, timeline browsing mode, and folder browsing mode) to browse photos and videos.
8	Timeline	Show/Hide the timeline.
9	Sort	Sort items chronologically in an ascending or descending order.
10	Add Album	Create an album or smart album.
11	Photo/Video Filter	Display either photos or videos, or both.

12	Zoom in/Zoom out	Zoom in to enlarge the thumbnail size or zoom out to reduce the thumbnail size.
13	Background Color	Switch between a white and black background color.
14	Slideshow	Play selected items as a slideshow and click the down arrow to choose the slideshow speed, effect and background music.
15	Import	Import videos or photos.
16	Download	Download the selected photo or video. You can also select the resolution of the photo to download (if it is a video, then the resolution chosen is for its thumbnail.)
17	Share	Choose to share the selected items via email, on social networks, or via link. This will bring up Sharing Cart. For details on Sharing Cart, refer to the <a href="#">Sharing photos, videos, albums, or smart albums</a> section in this chapter.
18	Multi-Select	Select multiple items at the same time.

**Note:**

- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW system does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, please refer to the [Transcode Management](#) chapter.

**Left Panel**

- Shared Photos: List all photos and videos chronologically by their thumbnails (except photos and videos in the "/home" and "Qsync" folders) and all photos and videos are only visible to authorized users.
- Folder: Show the folders, photo and video files contained in a folder on the QGW system (except photos and videos in the "/home" and "Qsync" folders) and all photos and videos are only visible to authorized users.
- Private Collection: List all photos and videos located in the "/home" folder, and those multimedia files can be only viewed by yourself.
- Qsync: List photos and videos synchronized from the Qsync service.

- Album: List all virtual albums. Note that all entries listed under an album are only links to files. This can effectively conserve your QGW system storage space, as you can keep only one copy of the photos even if you create an album for a special theme. You can also right click on "Album" (the category header) to expand/collapse the album list or add an album. For album operations, please refer to the section on [Creating and managing albums](#) below.
- Smart Album: List all smart albums. Smart albums will only show photos or videos that match specific conditions chosen by users, such as today in history, random, tag and all files and can save you effort in managing photos. You can also right click on "Smart Album" (the category header) to expand/collapse the smart album list or add an album. For instructions on smart album operations, please refer to the [Creating and managing smart albums](#) section.
- Shared Center: Show the photo and video sharing history. You can check the name, link, expiration date and summary of each record and choose to re-share the shared items. You can also right click on "Shared Center" (the category header) to expand / collapse the album list.
- Faces: List albums containing photos with face tags. Please refer to the [Adding face tags to photos](#) section for more details.
- Recently: Include recently-imported (within two months) photos and videos from local device or taken (within two months) with a camera or recording device.
- Trash Can: All deleted photos and videos can be found here and can be restored or permanently deleted. Only deleted files (and not virtual links) will show up in the trash can.

**Note:**

- The "/home" folder can only be accessed by its owner and QGW system administrators. Private or personal videos should only be stored in your "/home" folder.
- For media folder configuration, refer to the [Multimedia Management](#) chapter. For user setup and configuration, refer to the [User](#) section in the Privilege Settings chapter.
- If uploaded photos or videos do not show up in Photo Station, scan for them using the Media Library. For details on the scan, please refer to the [Multimedia Management](#) chapter.

## Using Photo Station

### Creating and managing albums

There are two ways to create an album:

1. Switch to the folder view in Manage mode, right click on a folder, and select "Create New Album" to turn that folder into an album.
2. Drag & drop photos or videos in "Album" on the left panel.
3. Right click on "Album" on the left panel > "Add Album" and specify to share the album with QGW system users or with the public (if an album is shared with the public, photos in that album will be shown on the QTS Gateway login screen.)

To manage albums, right click on an album and choose to download, remove, rename, share, stream, play as a slideshow, open, or configure its settings.

### Creating and managing smart albums

Similar to an album, there are three ways to create smart albums:

1. Switch to the folder view in Manage mode, right click on a folder and you will see two smart album options: "Create a Smart Album" and "Convert subfolder to Smart Album". Select "Create a Smart Album" to turn that folder into a collective smart album. Select "Convert subfolder to Smart Album" and all the subfolders within that selected folder will become individual smart albums under "Smart Album" on the left panel.
2. Drag & drop photos or videos in "Smart Album" on the left panel.
3. Right click "Smart Album" on the left panel > "Add Album" and choose the sharing options, file type, source path, and search criteria > Click "Create".

To manage smart albums, right click on an album under "Smart Album" in the left panel and choose to download, remove, rename, share, stream, play as a slideshow, open, or configure its settings.

### Sharing photos, videos, albums, or smart albums

You can share photos, videos, albums, or smart albums with your friends via email, social networks, or sharing links using Sharing Cart or configure sharing settings when you create an album or smart album.

### Sharing Cart

Sharing Cart allows you to conveniently collect photos and videos stored in different albums or folders before sharing them. After you collect items using Sharing Cart, choose one of these methods to share them:

- Email: Complete required fields (including sender email, recipient emails, password, valid period, subject and message (in "More settings") and click "Create".  
**Note: To share files/folders using your own email account, please first set your email account in QTS Gateway Desktop > "Options" > "E-mail Account".**
- Social network: Complete required fields (including shared way, social network, message, domain name), choose to use SSL, set the password and valid period and click "Create".
- Sharing link: Choose the link format and whether to create a secure link using SSL, set the password and valid period and click "Create".

Note that for album or smart album, all the photos/videos within that album will be loaded to Sharing Cart, while for a photo or video, only that item is loaded.

## Configuring sharing settings

As you create an album, you can choose to share it with other QGW system users (choose whether all QGW system users can edit the album, or only the album creator/administrator can edit the album) or the public (show this album on the QTS Gateway login page - please note that this option is only available for administrators) or not to share at all (leave both options unchecked), and set the valid period on the album creation page.

## Checking sharing history

To check the sharing history, click "Shared Center" on the left panel in Manage mode. You can review the details of a record or re-share the shared items.

### Note:

- As a Photo Station administrator, you can also share a public album on the login screen (the photo wall style login screen can be set in "Control Panel" > "General Settings" > "Login Screen".)
- If an album is set to share with the public, users can click the photo wall on the login page to check the album.
- An exclamation mark will appear on the album thumbnail if the sharing period of that album has expired.

## Photo and Video Operations

After right clicking on a photo or video in Manage mode, a menu will show up, and users can choose to perform a desired action from the list.

Operation	Description
Rotation(counter-clockwise rotation icon)	Rotate the photo 90 degrees counter-clockwise (photos only.)
View (eye icon)	Launch the media viewer to view the photo (photos only.) Refer to the <a href="#">Viewing photos and videos</a> section for more details.
Information (i)	Display file details, properties and a description of the photo (photos only.)
View	Launch the media viewer to view the photo (photos only.) Refer to the <a href="#">Viewing photos and videos</a> section for more details.
Rotation(clockwise rotation icon)	Rotate the photo 90 degrees clockwise (photos only.)
View/Play	Launch Media Viewer and play the selected item.

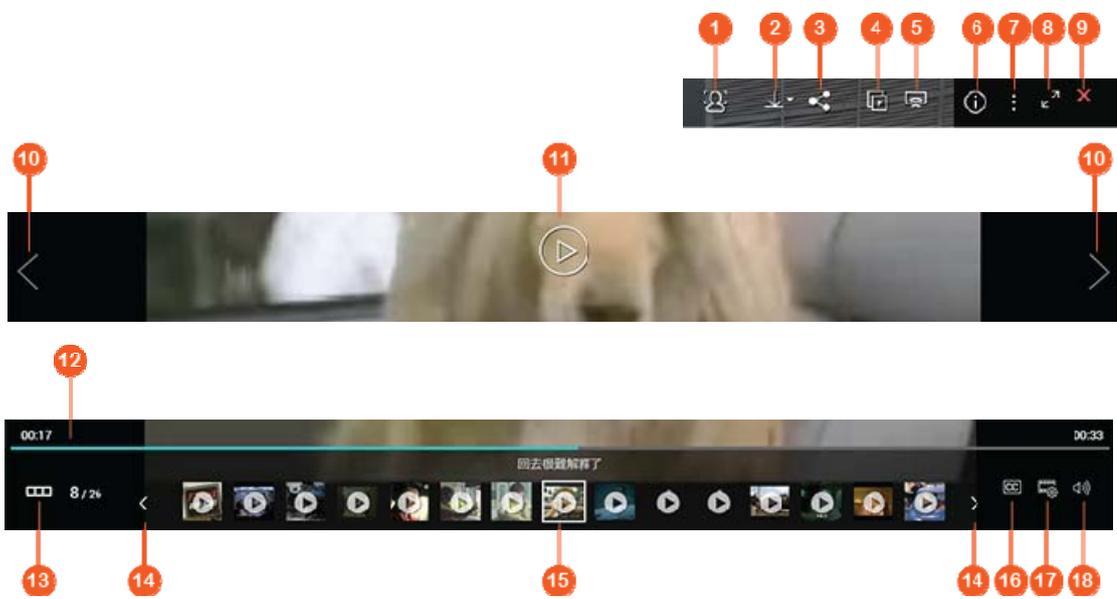
Open in new browser tab	Play the video or photo in a browser window.
Open with VLC	Play the video in a browser window (videos only; the VLC plug-in must be installed.)
Streaming to (Network Media Player)	Stream videos to compatible devices in different rooms over your home network.
Share	Share the photo or video on social networks, via email or link.
Download	Download the photo or video. For photos, there are four sizes: small, medium, large and original; for videos, you can choose to download the video file (please choose "Original") or video thumbnail (please choose "small", "medium", or "large".)
Add to Album	Copy the photo and video to an existing album or create a new album and then copy the item to that new album.
Add to Transcode	Convert the video to the following resolutions: 240P, 360P, 480P SD, 720P HD and 1080P Full HD (videos only.)
Edit	Edit the photo online using Pixlr Editor or Pixlr Express (photos only.)
Rebuild thumbnail	Rebuild thumbnail for selected photos or videos.
Delete	Delete photos or videos.
Information	Display file details, property and description of the photo/video.
Set Coordinates	Set GPS information of a photo (photos only.)
Add Tag	Add a tag to photos or videos.
Rating	Rate photos or videos.
Color Label	Color-label photos or videos.

### **Finding your photos and videos quickly**

You can rate or classify photos/videos to quickly locate them. To do so, right click on a photo or video and then tag, rate or color label them. To batch mark or classify multiple photos or videos, first click the "Multi-select" button on the main menu (or hold the Ctrl key), select your desired photos or videos and right click the photos or videos to perform desired actions. After photos or videos are tagged, rated, or color labeled, they can be searched by their rating, color label or tag in the search bar.

### **Viewing photos and videos**

In Gallery mode, double click on a photo or video or click the "Display" button in the thumbnail display style to launch the Media Viewer for viewing operations.



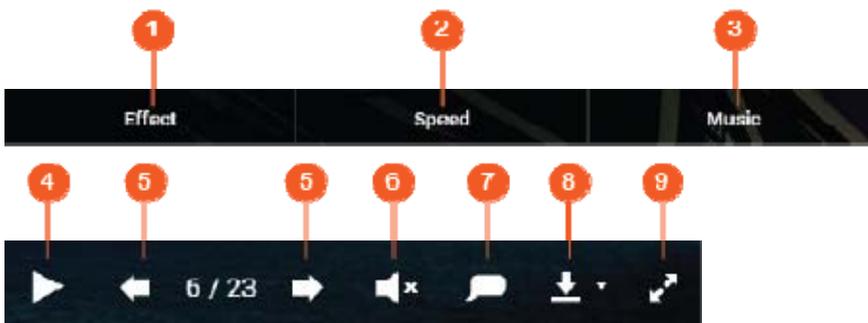
No	Name	Description
1	Face Detection	Enable Face Detection to show tagged faces. You can also manually add a face tag. Please refer to the <a href="#">Adding face tags to photos</a> section for more details.
2	Download	Download the photo or video. For photos, there are four sizes: small, medium, large and original; for videos, you can choose to download the video file (please choose "Original") or video thumbnail (please choose "small", "medium", or "large".)
3	Share	Share the photo or video image on social networks, via email or link.
4	Slideshow	Play the photos/videos in this album as a slideshow in full screen mode. Check the <a href="#">Playing photos and videos as slideshow</a> section for more details.
5	Network Media Player	Stream videos to compatible devices in different rooms over your home network.
6	Information	Display file details, property and description of the photo/video.
7	Miscellaneous Settings	Set the currently displayed photo/video image as QTS Gateway wallpaper.
8	Full Screen	View the photo or play the video in the full screen mode.
9	Return to Photo Station	Close the photo/video viewer and return to Photo Station.

10	Last Item/Next Item	Play the last/next item.
11	Play/Pause	Play the photo/video as slideshow.
12	Seek Bar	Control the playback progress.
13	Hide/Show Preview Bar	Hide/show the Preview Bar.
14	Rewind/Forward	Rewind/Forward the Preview Bar.
15	Preview Bar	Preview the photos and choose which photos or videos to preview next.
16	CC (available when the item opened is a video)	Display and adjust subtitles.
17	Resolution (available when the item opened is a video)	<ul style="list-style-type: none"> <li>Switch the resolution for the played video (Only available if your QGW system model supports On-the-fly transcoding.)</li> <li>Watch the video in another browser page or with VLC.</li> </ul>
18	Volume (available when the item opened is a video)	Adjust the player volume.

**Playing photos and videos as slideshow**

A slideshow is a collection of photos that are played in a sequential fashion at an interval in full screen mode for your photo enjoyment. To play photos or video images as slideshow, click the "Slideshow" button in Gallery mode to switch the viewing mode.

Use the buttons on the menu bar for slideshow or album operations.



No	Name	Description
1	Effect	Set a different slide transition effect.
2	Speed	Set the slide speed.

3	Music	Switch between different playlists defined in the Music Station (from the "Playlist", personal playlist and shared playlist on the left panel.)
4	Play/Pause	Play/Pause the slideshow.
5	Last/Next Slide	Go to the last/next slide.
6	Background Music	Turn the background music on or off.
7	Title	Show the photo title.
8	Download	Choose to download the current photo or every photo in the slideshow in large or original image size.
9	Full Screen	Switch between full screen and windowed modes.

### Geotagging photos and photo map

To geotag a photo, right click on a photo and select "Set Coordinates" to set its coordinates (you can either type the coordinates or the location in the search box in the "View Map" dialog window.) Click "Save" after you finish the setting. To view photos on a map, click on the photos > "Information", and then click the red pin next to "Coordinates". This feature is only available for photos with GPS coordinates. For photos with no GPS coordinates, please follow the above steps to set their GPS coordinates.

### Adding face tags to photos

1. Set face detection folders in Photo Station > "Manage Mode" > "Settings" > "Face Detection".
2. Open a photo in the Media Viewer and enable Face Detection.
3. Add face tags to the photo, or manually change the face area.

To view photos with face tags, switch to Manage mode and click "Faces" on the left panel.

### Browsing PDF files

You can also browse PDF files as photos using Photo Station. To use this feature, right click on a PDF file to create a new album. After clicking on that album, you will see all the pages of the PDF file displayed as individual photos.

#### Note:

- Before using the Face Detection and PDF browsing features, the Photo Station Extension App must first be installed in the App Center.
- As the face detection function can affect system performance, avoid using it during peak usage periods.

## Media Library and Privacy Settings

Photo and video files in Photo Station are listed and displayed according to shared folder privileges and media folders settings in the [Media Library](#). For shared folder privileges, only users with an appropriate permission to a shared folder can view its contents in the Photo Station. For example, if a user does not have read/write, or read-only permissions to a certain shared folder, that user cannot see the photos and videos in the shared folder.

### Note:

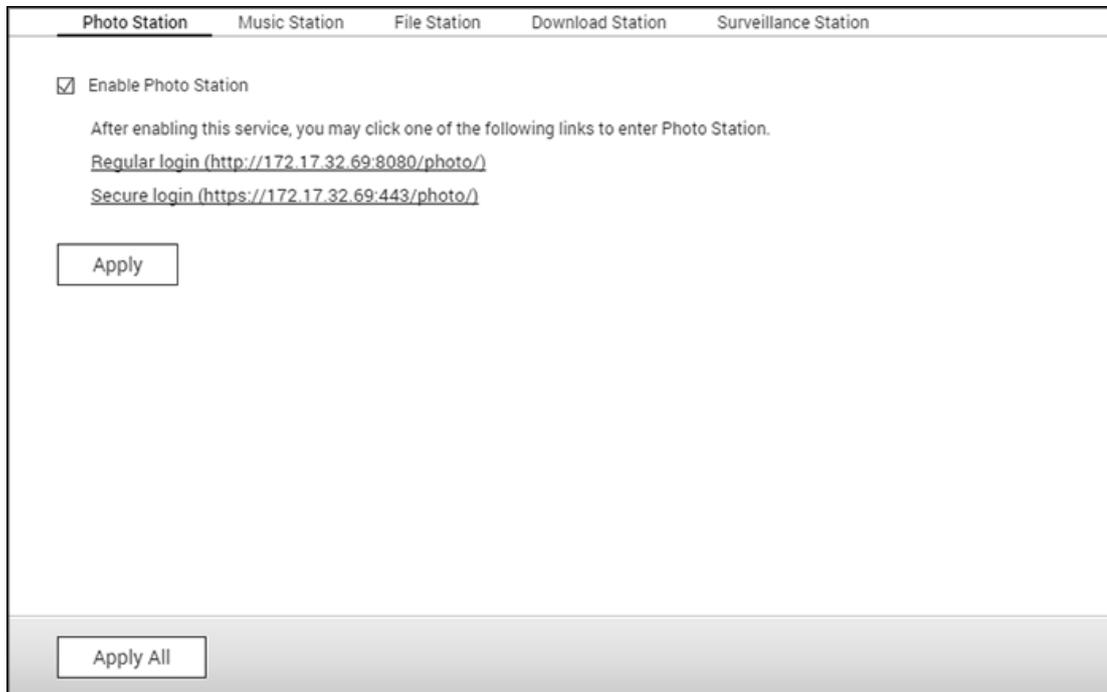
- In addition to shared folder privileges, you can also store private videos in your "/home" shared folder to hide them from other QGW system users (except the administrator.) The contents of the "/home" folder can be found under "Private Collection". Anyone attempting to access this folder in Photo Station will be prompted for a password.
- To create a shared folder, go to "Control Panel" > "Privilege Settings" > "Shared Folders".

Photos and videos stored in the shared folders are only visible after they are detected and scanned by the Media Library. To set the Media Library to scan for photos and videos manually or by schedule go to "Control Panel" > "Multimedia Management" > "Media Library". For more details on media folder settings, please refer to the chapter on Multimedia Management.

**Note:** As the media folders in the Media Library are shared by Photo Station, Video Station and DLNA Media Server as their content source, content will be affected in those applications if new media folders are added or existing media folders are removed from the Media Library.

# Station Manager

The Station Manager is an integrated control panel for all QNAP Stations and they can be enabled or disabled here.



## Enabling Photo Station

Check "Enable Photo Station" and click the below links to directly login to the application. Check "Show the photos of Sharing Management on the login screen" to display photo albums on the login page. This will allow users to directly view the photos of the chosen album as a guest. Photo Station can only be launched after it is enabled in the Station Manager. For more Photo Station details please refer to the [Photo Station](#) chapter.

## Enabling File Station

Check "Enable File Station" and click the below links to directly login into the application. File Station can only be launched after it is enabled in the Station Manager. For more File Station details please refer to the [File Station](#) chapter

## Enabling Download Station

Check "Enable Download Station" and click the below links to directly login to the application. Download Station can only be launched after it is enabled in the Station Manager. For more Download Station details please refer to the Download Station [Download Station](#) chapter

## Enabling Surveillance Station

Check "Enable Surveillance Station" under "Settings" and click the below links to directly login to the application. Surveillance Station offers two free recording channel. To add extra recording channels, please purchase a license from the QNAP License Store (<http://license.qnap.com>) or contact an authorized reseller in your region for details.

### Note:

- The maximum number of recording channels supported is for reference only. The actual recording performance may vary depending on the IP cameras, video content, network bandwidth, recording settings, and other applications running on the QGW system. Please contact an authorized reseller or camera vendors for more information.
- For a step-by-step tutorial on adding extra channels, please refer to [https://www.qnap.com/i/en/trade\\_teach/con\\_show.php?op=showone&cid=49](https://www.qnap.com/i/en/trade_teach/con_show.php?op=showone&cid=49).
- Windows users are advised to use IE 10+, Chrome or Firefox for live view and playback.
- Mac users are recommended to use the Surveillance Client for Mac for live view and playback operations. Surveillance Client for Mac can be downloaded from <http://www.qnap.com/download>.

To check on license details, switch to the "License Management" page.

# Transcode Management

Transcoding is the process of converting video files into an universal format (\*.MP4) that is compatible with the broadest range of media players such as mobile devices and Smart TVs. Converted files with a range of resolutions can be used across different network environments for a better viewing experience. After transcoding tasks are created, they can be managed here. The transcoding service is enabled by default.

On-the-fly Transcoding Task    **Background Transcoding Task**    Auto Transcoding Folder

Transcode function provides video conversion for you to play videos smoothly from different devices. You can convert a video through File Station, Photo Station, or Video Station.

Hardware accelerated transcoding: None

Current Status: **Transcoding**

Manually-added first

Unfinished

File name	Size	Durati...	Resoluti...	Transcod...	Start Ti...	Finish T...	Time ...	Sta
00. OST Par...	66.2 ...	00:03:...	1920x1...	360p	2015/12...	--	--	Trai
(( Secret W...	478.4 ...	00:03:...	4096x2...	360p	--	--	--	Sta

## On-the-fly Transcoding Task

On-the-fly transcoding will simultaneously convert and stream a video while you watch it. This will consume more CPU resources. If your QGW system has hardware transcoding acceleration, it is recommended to install the CodexPack to increase transcoding speeds and reduce CPU load. You are able to view and manage who is using on-the-fly transcoding services.

Manage transcoding tasks using the following buttons:

Button	Name	Description
	Refresh	Refresh the list.

Manage each task with the following buttons:

Button	Name	Description
	Priority	Adjust the order each task is executed.

	Remove	Remove the selected task from the list.
---	--------	---

### Background Transcoding Task

Background transcoding is when a video file is converted in advance, potentially avoiding high CPU usage if the video will be simultaneously accessed by many users. You can manually add videos to be transcoded using File Station, Photo Station, or Video Station. Video files can be converted to 240p, 360p, 480p, 720p and 1080p and will be saved in the "@Transcode" folder that is in the same directory as the video.

Manage all transcoding tasks using the following buttons:

Button	Name	Description
Stop Transcoding	Stop Transcoding	Suspend all ongoing tasks in the list.
Remove All Incomplete Tasks	Remove All Incomplete Tasks	Remove all tasks that are yet to finish from the list.
Remove All Complete Tasks	Remove All Complete Tasks	Remove all complete tasks from the list.
Refresh	Refresh	Refresh the list.

Manage each task with the following buttons:

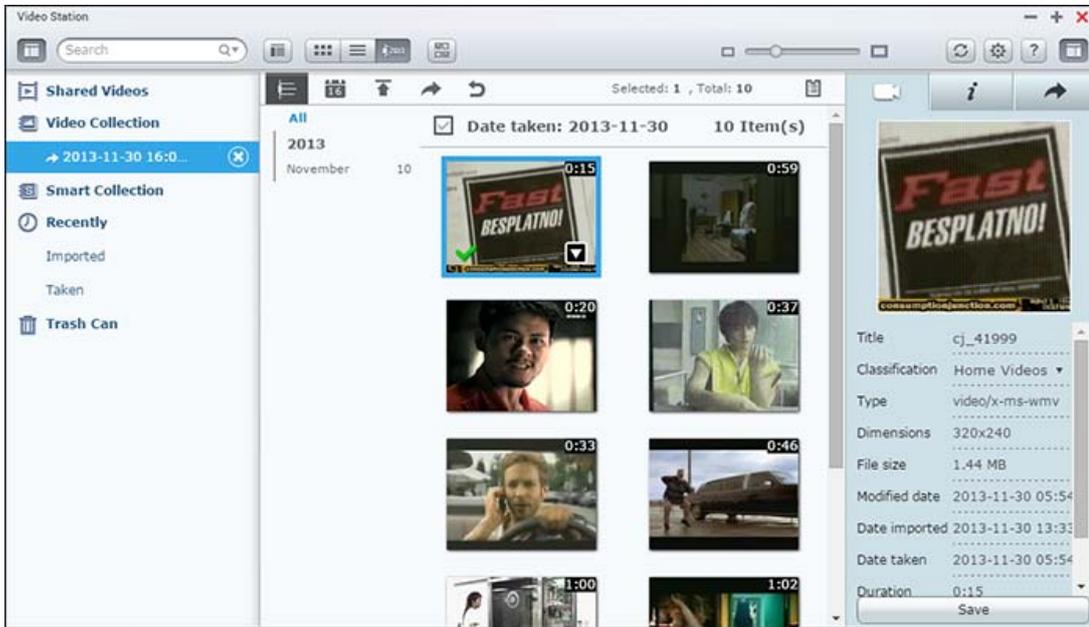
Button	Name	Description
	Priority	Adjust the order each task is executed.
	Remove	Remove the selected task from the list.

### Auto Transcoding Folder

This feature is designed to convert the contents of an entire folder, and within the folder, the resolution of each subfolder can be specified independently. Click "Add" to add a new folder and select the video quality (resolution) and the folder to add it to the task list.

# Video Station

Video Station (2.3) is a video management tool used to organize videos on the QGW series and to share them with others across the Internet. With Video Station, you can classify videos into home videos, movies, TV shows or music videos for personal collections. Smart collections can be set to automatically sort videos that match certain criteria and help you neatly manage your videos.



This chapter covers the following topics:

- [Starting Video Station](#)
- [Familiarizing yourself with Video Station](#)
- [Using Video Station](#)
- [Media Library and Privacy Settings](#)

## Starting Video Station

Install and enable Video Station from the App Center (for QTS Gateway 4.2 or later) and follow these steps:

1. Upload videos to a shared folder on the QGW series: You can upload videos to the QGW series in 3 different ways: 1) Install Qfinder Pro on your PC or Mac, set up a network drive and upload files to your preferred shared folders. For details on setting up a network drive, please "[Connecting to Shared Folders](#)"; 2) Click "Shared Videos" or "Private Collection" on the left panel and "Import" (up arrow) on the main menu to import videos from the local PC. A new shared folder with the date that files are uploaded will be created on the QGW series to store uploaded files (for "Shared Videos", this newly-created shared folder is located under the "/multimedia" folder; for "Private Collection", this shared folder is located under the "/home" folder.) A corresponding collection will be created under "Video Collection" as well; 3) Switch to folder view browsing mode and drag &

drop videos to a preferred folder. With the first and third approach, you can choose which folder on the QGW series that you want to upload videos to.

**Tips on file upload:**

- The maximum size of an image file is 2GB.
- The maximum size of multiple files that can be uploaded at one time is 2GB.

2. Launch Video Station from the Main Menu/Desktop shortcut, or directly log into Video Station by going to: [http://QGW\\_Name\\_or\\_IP/video/](http://QGW_Name_or_IP/video/)

**Note:**

- Admin login credentials of Video Station is the same as that of the QGW system administrator.
- Video Station supports: API, MP4, and more.

### Familiarizing yourself with Video Station

#### Menu Bar



No	Name	Description
1	Left Panel	Hide/Show the left panel.
2	Search Bar	Search video files by title, video date, tag, rating, or color label.
3	Browsing Mode	Switch between different browsing modes (from left to right: thumbnail browsing mode/list browsing mode/timeline browsing mode/folder browsing mode) to browse videos.
4	Multi-select	Select multiple items at the same time.
5	Resizing Bar	Resize video thumbnails.
6	Select DLNA/AirPlay Player (Network Media Player)	Locate compatible devices in different rooms over your home network.

7	Refresh	Refresh the current page.
8	Settings	<p>Set video classification, content filters, or social network binding; configure subtitles searching settings and miscellaneous settings.</p> <ul style="list-style-type: none"> <li>• Video Classification: Add, remove and rescan folders to be classified and classify folders into the following categories (Home Videos, Movies, TV Shows, or Music Videos), or manage your custom classifications. The classified videos will be organized into a video library for smart collections.</li> <li>• Content Filter: Set folders as the content source of Video Station. Use this feature to hide undesired videos and only show intended contents.</li> <li>• Social Network Binding: bind your social network accounts to share videos on social networks (more on this in the below "Sharing collections" section.)</li> <li>• Search Subtitles: Enable Video Station to search for subtitles on subtitles websites (including OpenSubtitles and Shooter.)</li> <li>• Miscellaneous: Check "Always ask me to enter my password when accessing Private Collection and Qsync", and each time a user is trying to access those categories, that user will be prompted for a password.</li> </ul>
9	Help	Check online help, quick start guide or version information.
10	Right Panel	Hide/Show the right panel.
11	Timeline	List videos chronologically in a timeline.
12	Date Filter	Filter videos by date.
13	Import	Import videos.
14	Sharing	Choose to email, publish, or share the link of a collection.
15	Return	Return to the root level of the "Video Collection" or "Smart Collection" when you are in your created collection.
16	Sharing History	Show the history of files that have been shared.
17	Tag Filter	Filter videos by tag.

**Note:**

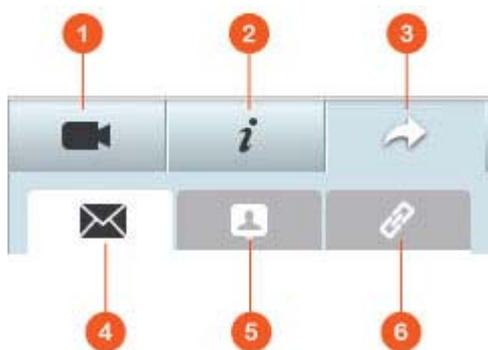
- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW system does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable. For details on transcoding, please refer to the [Transcode Management](#) chapter.
- If your QGW series supports transcoding, please install the CodexPack App before using this function. The QGW series will try to transcode to a suitable format for your device. If your QGW series does not support transcoding, the QGW series will only output the original file format and the seek function may not work properly. In this case, please make sure that your device is compatible with the file format used by the video. Some video formats may experience issues when streaming via DLNA, Apple TV or Chromecast. If any of these issues arise during video playback, you can consider transcoding your videos into universally-compatible media formats. For more details on transcoding, please refer to the [Transcode Management](#) chapter. Some media players do not support pausing during playback. If this happens, playback will continue even if you use the pause feature.

**Left Panel**

- Shared Videos: List all the videos in all shared folders on the QGW series (except videos in the "/home" and "Qsync" folders) and all videos are only visible to authorized users.
- Private Collection: List all videos located in the "/home" folder, and those multimedia files can be viewed by yourself only.
- Qsync: List videos synchronized from the Qsync service.
- Video Collection: List all virtual collections. All entries listed under a collection are only links to the physical files. This can effectively conserve your QGW system storage space, as you can keep only one copy of the videos even when you create a collection for a special theme. For collection operations, please refer to the below section on Using Video Station.
- Smart Collection: List all smart collections. Smart collections will only show videos that match user-defined classifications, such as Home Videos, Movies, TV Shows and Music Videos; and can save effort in managing videos. For instructions on smart collection operations, please refer to the section on Using Video Station below.
- Recently: Include recently-imported videos (within a month) from a local device or taken with a camera or recording device.
- Trash Can: All deleted videos can be found here and can be restored or permanently deleted. Only deleted files (and not virtual links) will show up in the trash can.

**Note:**

- The "/home" folder can only be accessed by its owner and QGW system administrators. Private or personal videos should only be stored in your "/home" folder.
- For media folder configuration, refer to the Multimedia Management chapter. For user setup and configuration, refer to the [User](#) section in the Privilege Settings chapter.
- If uploaded videos do not show up in Video Station, scan for them using the Media Library. For details on the scan, please refer to the [Multimedia Management](#) chapter.

**Right Panel**

No	Name	Description
1	Video Property	Review and edit video properties.
2	Tag and Description	Edit and browse video tags and descriptions.
3	Sharing	Drag files to this area and share them via a link (including three methods: email, social sharing and link.)
4	Email	Share a link via email. Specify the sender, recipient, subject and message body of the email and click "Send" to send the email. Make sure your email account is properly configured in QTS Gateway Desktop > "Options" > "E-mail Account".
5	Social Sharing	Share a link of selected files on social networking sites. Specify the subject and message body and click the social network icon to share.
6	Link	Share a link of selected videos by directly pasting it into an email or instant message. Drag and drop videos under "Select Videos" and under "Select Link Format", select the domain name, LAN IP or WAN IP address (note that the myQNAPcloud.com domain name is only available after it is registered in myQNAPcloud. Please refer to the <a href="#">myQNAPcloud</a> chapter for more details) and HTML format (click to

		choose a URL link, HTML code, vB Forum code or Alt Forum code) from the drop down menu. Click "Create", specify the name of the collection displayed on the page seen as recipients open the link. Copy and paste the URL link in the dialog window to your preferred applications.
--	--	---

**Note:** Multiple video files can be classified at the same time. To do so, select the video files, click "Video Property" on the right panel and choose their classification from the classification drop down list.

## Using Video Station

### Creating and managing collections

Collections can be created in two ways:

1. Switch to the folder view, right click on a shared folder, and select "Create New Collection" to turn that shared folder into a collection.
2. Drag & drop videos in "Video Collection" on the left panel.

Right click on a collection and choose to play, download, remove, rename, email the link of, publish the link, share the link of that collection, or modify the settings of that collection (the email, publish and share options are only available if "Share with the public" is enabled in "Collection Settings".)

### Creating and managing smart collections

To create a smart collection, click "+" next to "Smart Collection", specify the name of the collection, the classification (Home Videos, Movies, TV Shows and Music Videos) and search criteria (all files and tag.) Right click on a smart collection and choose to play, download, remove, rename, or reset collection settings. Right click on a smart collection and choose to play, download, remove, rename, email the link of, publish the link, share the link of that collection, or modify the settings of that collection (The email, publish and share options are only available if "Share with the public" is enabled in "Collection Settings".)

### Sharing collections

As you create a collection, you can choose to share it with other QGW series users (choose whether all QGW series users can edit the collection, or only the creator/administrator) or the public, or not to share at all (leave both options unchecked), and set the valid period on the collection creation page. If a collection is set to be shared with the public, you can right click on the collection and select "Email" to email it, "Publish" to publish it on social networks, or "Sharing Links" to generate and paste the collection link on your blog, forum, or instant messengers. You can still edit the collection content later, and the updated content will be presented when viewers click the same link.

You can also share a number of videos as you do with collections. To do so, click "Sharing" on the right panel, drag videos from different collections and drop under "Select Videos" on the right panel and use the "Email", "Social Sharing", or "Link" button to share the videos. Then, your friends can log into Video Station with the link provided to them to watch videos from shared collections. To check the sharing history of a selected collection, click on the collection and then on "Sharing History" in the main menu.

**Note:** To share files/folders using your own email account, first set your email account in QTS Gateway Desktop > "Options" > "E-mail Account".

## Video Operations

Right click on a video and choose to perform an action from the table.

Operation	Description
Play	Play the video online in the browser.
Open with VLC	Play the video in a browser window with the VLC player (please install the VLC plug-in first.)
Download	Download the video.
Copy to Collection	Copy the video to a collection.
Set as Cover	Set the video thumbnail as the cover of a collection.
Add to Transcode	Convert the video to the following resolutions: 240P, 360P, 480P SD, 720P HD and 1080P Full HD.
Rotate	Rotate the video 90 degrees clockwise or counter-clockwise
Add to Sharing List	Add the selected videos to the sharing list.
Streaming to	Stream videos to compatible devices in different rooms over your home network.
Remove/Delete	Delete the video.
Movie Information	Review movie information (such as genre, director, cast, etc) of the selected video.
Add Tag	Tag the video.
Rating	Rate the video.
Color Label	Color-label the video.

**Note:**

- The movie information option is only available after the video selected is classified as "Movies". Click the video property button on the right panel and the classification drop down menu to classify a video.
- Information is retrieved from the Internet based on the English title of video files. If the movie information is incorrect, modify the English title to retrieve the movie information.
- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Bonjour must be enabled when using multi-zone streaming. You can enable Bonjour in "Control Panel" > "Network Service" > "Service Discovery" > "Bonjour".
- Only MP4 video files can be directly streamed if your QGW series does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable.

**Finding your videos quickly**

To quickly locate videos, you can rate or classify them. To do so, right click on the videos and then tag, rate, or color label them. To mark/classify multiple videos, click the "Multi-select" button on the main menu (or hold the Ctrl key on the keyboard), select your desired videos and right click the videos to rate or classify them. After videos are tagged, rated, or color labeled, they can be searched by their rating, color label or tag in the search bar on the Main Menu.

**Viewing videos**

Double click on a video to switch to the video viewing mode and use the buttons to view videos:



No	Name	Description
1	Play/Pause	Play/Pause.
2	Stop	Stop playback.
3	Seek Bar	Control the playback progress.
4	Mute/Volume	Mute/Unmute and adjust the volume.
5	Resolution	Change resolution and transcoding settings.
6	Subtitles	Manage subtitles of the video.
7	Streaming to	Stream videos to compatible devices in different rooms over your

		home network.
8	Full Screen	Switch to the full screen mode.

**Note:**

- For HD videos, click the HD icon on top of the player window to switch video quality.
- You can *αλσο* control the playback and volume with your computer keyboard:
  - Left: Rewind
  - Right: Forward
  - Up: Increase volume
  - Down: Decrease volume
  - Space: Play / Pause
- To stream media files to HDMI or Chromecast using the Network Media Player, the Media Streaming Add-On must first be installed in the App Center.
- Only MP4 video files can be directly streamed if your QGW series does not support On-the-fly Transcoding. You can consider transcoding them into different media formats if they are desirable.

**Downloading and searching movie information online**

Video Station supports downloading online information (movie poster, year, rating, director, etc) for movies. To enable this feature, follow these steps:

1. Classify a video as movie (right click on a video > "Information" > change the Classification to "Movies" under the "Video Property" tab.)
2. Switch to the "Movies" category on the left panel.
3. Right click on a movie > "Movie information" to open the movie information page for that movie.
4. If the video information downloaded from the Internet is incorrect, click the "Edit" icon in the top-right corner of the "Movie Information" page and enter the movie keyword to search again. Please note that this feature only supports English keywords.
5. If the movie poster is incorrect, you can change it by clicking the "Edit" icon on the movie poster to upload it from your PC or via URL, or restore it to the default poster.

**Importing, displaying and adjusting subtitles**

You can import, display and adjust subtitles files for movies.

- To import and display subtitle files:
  - a. Save the subtitles file in the same directory as the video file, with an identical filename (for example, a video with the filename "video.avi" must have subtitle files named "video.eng.srt" or "video.cht.srt".) The subtitles will then be available to use when watching the video and you can switch between multiple languages.

- b. In the video player, click "CC" on the player panel > "Import subtitles" and choose the subtitles file from a computer.
- c. In the video player, click "CC" on the player panel > "Search for subtitles" and the system will search for subtitles based on the video information or by keywords. Select one of the results and the system will display the subtitles.
- Adjust Subtitles: In the video player, click "CC" on the player panel > "Adjust subtitles" to change the subtitles font, size, color or enable background effects. Or, make subtitles display earlier or later if they are not synced with the audio.

**Note:**

- "Import subtitles" and "Search for subtitles" are only supported from firmware 4.2.0.
- Supported subtitles file formats: .srt, .ass and .ssa.
- If your subtitles use an incompatible format, we recommend using Aegisub to convert them.

## Media Library and Privacy Settings

Videos in Video Station are listed and displayed according to shared folder privileges and media folders settings in the [Media Library](#). For shared folder privileges, only users with an appropriate permission to a shared folder can view its contents in the Video Station. For example, if a user does not have read/write, or read-only permissions to a certain shared folder, that user cannot see the videos in the shared folder.

**Note:** In addition to shared folder privileges, you can also store private videos in your "/home" shared folder to hide them from other QGW system users (except the administrator.) The contents of the "/home" folder can be found under "Private Collection". Anyone attempting to access this folder in Video Station will be prompted for a password.

Videos stored in the shared folders are only visible after they are detected and scanned by the Media Library. To set the Media Library to scan for videos manually or by schedule go to "Control Panel" > "Multimedia Management" > "Media Library". For more details on media folder settings, please refer to the chapter on Multimedia Management.

**Note:** As the media folders in the Media Library are shared by Photo Station, Video Station and DLNA Media Server as their content source, content will be affected in those applications if new media folders are added or existing media folders are removed from the Media Library.

# Mobile Apps

A list of mobile apps has been developed to help users access their QGW series with their mobile devices. The following are a list of benefits that mobile apps can bring you:

- Automatically update photos from your phones on your trip: When on vacation, photos on your mobile device can be automatically uploaded to your QGW series, allowing you to focus on your photos instead of worrying about running out of space.
- Easily share large files with others: Sharing huge files is extremely easy with the mobile apps. Share them whenever and wherever you want.
- Browse files stored on your QGW series: Access your office documents (Word, PDF, or Excel) stored on your QGW series using your mobile device.
- Manage services on your QGW series with ease: Check the status of your QGW series or enable/disable application services remotely using your phone.

Topics covered in this chapter:

- [Qfile](#)
- [Qmanager](#)
- [Qnotes](#)
- [Qremote](#)
- [Qvideo](#)
- [Qphoto](#)
- [Qget](#)
- [Vmobile](#)
- [Vcam](#)

## **Qfile**

Qfile enables you to browse and manage the files on your QGW series from your mobile device.

Manage multiple QGW systems in different locations conveniently from your mobile device. A simple and intuitive interface makes management easy. Thumbnails help you identify file types at a glance and you can move, copy, rename, and delete files on your QGW system without needing a PC.

## **Download**



## Qmanager

Qmanager is a powerful management platform with a simple to use and intuitive interface that makes monitoring and managing your QGW system from mobile devices amazingly easy.

Monitor system information, such as CPU usage, memory usage, system event info, online users, backup status, download progress, and file transfers. Use "App Center" to turn application services on or off with a single click. Restart or shut down your QGW system remotely.

### Download



## Qnotes

Qnotes is a powerful digital notebook and workspace for organizing your to-do lists, shopping lists, lecture notes, meeting notes, and everything else you want to remember. Synchronize your notes across your devices so you can access them wherever you go. Add audio recordings or take a picture and save it to Qnotes to keep it for you. Enjoy peace of mind that your notes are securely stored, and available from anywhere.

You can easily share your notes with others. Work together with your friends, family, classmates, and colleagues. Share your notebooks with others for viewing or editing.

### Download



## Qremote

Qremote is QNAP's remote control for HD Station. Use Qremote to control HD Station from your mobile devices.

### Download



## Qvideo

Qvideo helps you enjoy the videos on your QGW system via your mobile devices at anytime, anywhere and also to share your videos with others.

### Download



## Qphoto

Qphoto helps you enjoy your personal photo collection on your mobile devices at any time, from anywhere, without limits. Relive and share your special moments on the go.

### Download



## Qget

Qget allows you to manage all of the download tasks on your QGW system using your mobile devices at anytime, anywhere. Use Qget to add and monitor your download tasks in Download Station. The Qget built-in browser helps you to add tasks from direct download links or from magnet links.

### Download



## Vmobile

Vmobile is a mobile video surveillance application that enables you to connect to and manage your video surveillance system from your mobile device at anytime from anywhere. Connect Vmobile to a QGW system with Surveillance Station installed and you can monitor IP cameras and play recordings. Monitor several servers/channels from all of your network cameras or by simply connecting to any available QGW system on the network.

### Download



## Vcam

Vcam can turn your mobile device into a network camera, allowing you to record any moment around you to your QGW system. Vcam provides a great way to deploy a home surveillance system without purchasing expensive IP cameras.

### Download



# Computer Utilities

IEI provides the following utilities to improve productivity:

- [Qfinder Pro](#)
- [myQNAPcloud connect](#)
- [Qsync 2.0](#)
- [NetBak Replicator](#)
- [Qget](#)
- [vSphere Client plug-in](#)
- [Qsnap](#)

## **Qfinder Pro**

Qfinder Pro is a utility, available for Windows, Mac, and Linux, to quickly find and access a QGW system on LAN. Install Qfinder Pro on your computer, open it, double click your QGW system, and the login page is ready for you.

[Download](#)

## **myQNAPcloud connect**

myQNAPcloud Connect helps you to quickly and securely access published services of your QGW system on the Internet. myQNAPcloud Connect is designed for Windows users. By installing myQNAPcloud Connect, you will be able to connect to the QGW system and easily manage files by drag & drop within the Windows File Explorer.

[Download](#)

## **Qsync 2.0**

Qsync is a file synchronization service. Simply add files to your designated sync folder(s) and those folders and files will be available on the QGW system and all devices linked to it.

[Download](#)

## **NetBak Replicator**

The NetBak Replicator helps you easily back up files from a Windows PC to the QGW system, including entire disk drives, documents, pictures, music, videos, fonts, emails, and more. The operation is very simple. You can carry out backup tasks in just a few clicks using by setting real-time synchronization, scheduled backup and auto-backup from multiple PCs to the QGW series.

NetBak Replicator also supports backing up to a remote server via FTP and WebDAV through the Internet.

[Download User Manual](#)

## **Qget**

QGet is a powerful utility for download management. The software is available for Windows and Mac computers, allowing the management of HTTP, and FTP download tasks of Download Station on multiple QGW systems.

[Download](#)

## **vSphere Client plug-in**

The QGW system supports vSphere Client Plug-in that allows managing VMware datastores on the QGW series directly from the vSphere client console. In a large-scale server virtualization environment, management is centralized and straightforward. Administrators can easily control the status of the QGW system and datastores and create additional datastores to multiple ESXi hosts in just a few clicks.

[Download](#)

## **Qsnap**

Qsnap is a handy utility that can assist in quickly capturing screenshots on your PC. They can be quickly edited, saved and shared allowing quick note-taking and productive communication.

[Download](#)

# NAS Add-ons

The following NAS Add-ons (QPKG) are recommended to help you explore other possibilities:

## Storage and Backup

- [Backup Versioning – Beta](#)
- [Gmail Backup -Beta](#)
- [Hybrid Backup Sync - Beta](#)

## Virtualization

- [Container Station – Beta](#)
- [Virtualization Station - Beta](#)
- [Linux Station - Beta](#)

## Productivity

- [Notes Station - Beta](#)
- [Qsirch – Beta](#)
- [Qmail Agent- Beta](#)

## Entertainment

- [Media Streaming Add-On](#)
- [Photo Station Extension - Beta](#)

## Security

- [L2TP/IPsec VPN Service](#)
- [MyQNAPcloud SSL Certificate](#)
- [Surveillance Station](#)
- [Proxy Server](#)

## Connectivity

- [CloudLink](#)

## Business

- [Signage Station](#)

## Tool

- [Diagnostic Tool – Beta](#)
- [Q'center](#)

## **Backup Versioning – Beta**

Backup Versioning enables version control option in RTRR backup jobs. When creating a RTRR backup job, the option "version control" is available and allows preserving a certain amount of versions, and also a smart version recycling to be able to retain backups longer time.

### **Gmail Backup -Beta**

Gmail backup provides Gmail backup and recovery functionality, allowing users to create individual backup or domain account backup tasks. Gmail can be backed up by schedule and the content previewed through a web management interface. Backed up mail can be restored to the original mail account or other accounts: just configure the restore account, enter the account and password and the user can restore mail to the specified account.

### **Hybrid Backup Sync - Beta**

Hybrid Backup Sync is a comprehensive data backup and disaster recovery solution for files stored on QGW system. It integrates backup, restoration and synchronization features to provide a variety of options for data backup and synchronization including USB one-touch backup, Time Machine backup, RTRR backup and synchronization through RTRR, Rsync, FTP, CIFS/SMB and various cloud services such as Amazon® S3, Amazon® Glacier, Azure™ Storage, Google Cloud Storage™, S3/OpenStack Swift/WebDAV compatible services, Google Drive™, Microsoft® OneDrive® and Dropbox®. Hybrid Backup Sync allows users to create storage, remote and cloud account settings in advance which can help save time in creating backup jobs.

### **Container Station – Beta**

Container Station integrates both LXC and Docker virtualization technologies. This enables the use of multiple, isolated Linux systems on the QGW system. We have also engineered one-click download, install, and deployment of thin applications from the built-in Docker Hub Registry to make virtualization easier than ever.

## **Virtualization Station - Beta**

Virtualization Station turns the QGW system into an appliance server, and allows you to install virtual machines (VMs) on the QGW system with Windows, Linux, UNIX and Android operating systems. It can increase the functionality of the QGW system and be eco-friendly by using VMs instead of physical servers. With an easy-to-use interface, you can centrally manage all of the VMs created on the QGW system with minimal effort. You can also access virtual machines remotely on PCs and mobile devices by using web browsers at anytime. Virtualization Station allows users to open the data on the QGW system directly through VMs, reducing bandwidth utilization and greatly enhancing data security as all of the actions are carried out within the QGW system and no data is transmitted externally. Running application services on VMs is also efficient and secure by leveraging the high-performance I/O and the comprehensive data protection of the QGW system.

## **Linux Station - Beta**

Linux Station is a standard Linux desktop platform that allows you to use QTS Gateway while simultaneously using Linux on an HDMI display. Simply connect a keyboard and mouse to the QGW system to use the QGW system as a PC. You can also enable the remote desktop connection to use Linux Station with a web browser.

## **Notes Station - Beta**

Notes Station enables you to create digital notebooks on the private cloud provided by the QGW system. You can also easily leverage the files, photos and videos stored on the QGW system to enrich your notes. With Notes Station, digital memos are safely kept for instant access. Notes Station provides a straightforward interface for note taking. You can easily insert all kinds of files stored on the QGW system as part of your notes or as attachment to enhance the content.

## **Qsirch – Beta**

With Qsirch you can enhance your productivity with a powerful full-content search. QGW series allows you to store huge amounts of data, files, and information. But it can be very easy for important files to get lost as increasing amounts of data is stored on it, making productivity suffer as users spend time searching for files instead of working. Qsirch can help users locate files in the shortest possible time. Qsirch has advanced file extraction and a near real-time search engine, allowing users to quickly search through the entire QGW system to find desired files as soon as possible. The unique TF-IDF algorithm actively predicts your results as you type for lightning speed.

## **Qmail Agent – Beta**

Qmail Agent is an online mail client that allows users to access all of their email accounts and switch accounts easily. Whether it's Gmail, Outlook, Yahoo!, or other IMAP and POP3 mailbox services, Qmail Agent supports them all. It provides complete functionality for composing, reading and organizing email messages. It can also attach files, photos and documents from the QGW series. Qmail Agent also works with Gmail Backup to review archived emails.

## **Media Streaming Add-On - Beta**

The Media Streaming Add-On is an add-on for stations in QTS Gateway (File Station, Photo Station, and Video Station) that allows you to stream your media to different devices in different locations simultaneously using AirPlay, DLNA, Chromecast, and HDMI-connected devices. With the advanced management of the DLNA Media Server, you can also set advanced settings, such as DLNA client control, menu language and more.

## **Photo Station Extension - Beta**

This Photo Station Extension App will enable the face detection\* and pdf album import features for your Photo Station. You will be able to browse the imported pdf files as albums easily on other mobile devices.

## **L2TP/IPsec VPN Service**

L2TP (Layer Two Tunneling Protocol) is a combination of the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F.) Compared to PPTP, which only establishes a single tunnel between the two end points, L2TP supports the use of multiple tunnels. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity checks. The combination of these two protocols provides a high-security VPN solution which is known as L2TP/IPsec. L2TP/IPsec is supported by most clients, including Windows, Mac, Linux, and mobile devices.

## **MyQNAPcloud SSL Certificate**

After installing the myQNAPcloud SSL Certificate App, you will see the user interface on QTS Gateway myQNAPcloud to download and install your purchased SSL certificates from the myQNAPcloud website (<https://www.myqnapcloud.com>.) SSL certificates bring better protection when connecting to your QGW series via myQNAPcloud DDNS.

## **Surveillance Station**

Surveillance Station is a professional network surveillance system and video management system. As one of the standard applications, the Surveillance Station can be activated on the App Center to turn your QGW series into a professional network video recorder. When used with compatible IP cameras, Surveillance Station can perform the following operations: real-time monitoring, recording, playback, alarm notifications, Intelligent Video Analytics and video management to help you secure your assets and property.

## **Proxy Server**

The Proxy Server application provides an intuitive interface to simplify proxy server settings on your QGW system, enabling you to operate your own proxy server in just a few clicks. The proxy server provides cache and connection controls for Internet services. For companies that need a boost to web response time and security, this application can be leveraged to make your QGW system a web proxy server to protect other devices in your local network from Internet attacks.

## **CloudLink**

CloudLink is the best remote access service provided by myQNAPcloud that allows you to connect to your device via the Internet using the myQNAPcloud website ([www.myqnapcloud.com](http://www.myqnapcloud.com).) No complicated port forwarding settings on the router are required: just install CloudLink App on device App Center and sign in myQNAPcloud ID (QID) on your device. Then you can access files from the myQNAPcloud website. CloudLink will select the best connection for you according to your network environment. In addition to the web-based connection, CloudLink also allows you to connect to your device with Mobile Apps Qfile, Qmanager and the PC utility Qsync. CloudLink makes remote connectivity so easy.

## **Signage Station**

Signage Station provides digital signage display functionalities and allows content to be managed with access permissions. Users can use iArtist Lite to design the digital signage content and upload to the QGW system, and use Signage Station to display the digital signage media content on the web browser from the QGW series.

## **Diagnostic Tool – Beta**

The diagnostic tool provides a variety of system analysis functions to check the stability of a QGW system. Users can export system kernel records for sending to technical support staff for further investigation and system kernel log analysis tools can quickly check if abnormal actions have occurred. There are also tools for checking the file system, hard drives and RAM to provide a simple way to test system reliability.

## **Q'center**

Q'center is a central management platform that enables you to consolidate the management of multiple QGW systems. The Q'center web interface gives you the ease-of-use, cost-efficiency, convenience and flexibility to manage multiple QGW systems, across multiple sites, from any internet browser.

# GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## **Preamble**

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## **TERMS AND CONDITIONS**

### 0. Definitions.

'This License' refers to version 3 of the GNU General Public License.

'Copyright' also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

'The Program' refers to any copyrightable work licensed under this License. Each licensee is addressed as 'you'. 'Licensees' and 'recipients' may be individuals or organizations.

To 'modify' a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a 'modified version' of the earlier work or a work 'based on' the earlier work.

A 'covered work' means either the unmodified Program or a work based on the Program.

To 'propagate' a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To 'convey' a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays 'Appropriate Legal Notices' to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

#### 1. Source Code.

The 'source code' for a work means the preferred form of the work for making modifications to it. 'Object code' means any non-source form of a work.

'Standard Interface' means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The 'System Libraries' of an executable work include anything, other than the work as a whole, that:

- a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and
- b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A 'Major Component', in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The 'Corresponding Source' for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

## 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

## 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

## 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to 'keep intact all notices'.
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an 'aggregate' if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

## 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A 'User Product' is either (1) a 'consumer product', which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, 'normally used' refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

'Installation Information' for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor

any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

## 7. Additional Terms.

'Additional permissions' are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient,

for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered 'further restrictions' within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

#### 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License

grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

#### 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An 'entity transaction' is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

#### 11. Patents.

A 'contributor' is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's 'contributor version'.

A contributor's 'essential patent claims' are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, 'control' includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a 'patent license' is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or

covenant not to sue for patent infringement). To 'grant' such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. 'Knowingly relying' means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is 'discriminatory' if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

## 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

### 13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

### 14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License 'or any later version' applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

### 15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

### 16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS

PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS