QNE Network 1.0.x

User Guide

Document Version: 9
06/07/2023

Contents

4. Network Manager

5. Service Composer

6. myQNAPcloud

7. AMIZ Cloud

8. HybridMount

9. File Station

13. HA Manager

14. Application Store

15. Licenses

16. QuLog Center

17. Notification Center

18. Security Center

19. QuFirewall

20. Resource Monitor

21. Helpdesk

22. Console Management

1. Overview

This overview introduces the basic concepts and operations of QNE that can help familiarize users with QNE.

About QNE Network

QNE Network is a Linux-based operating system designed for edge computing. The system runs applications for cloud management and virtualization to provide network services. The optimized kernel and various services efficiently manage system resources, support applications, and protect important data. QNE Network also provides built-in utilities that extend the functionality and improve the performance of the device.

The multi-window, multitasking user interface facilitates the management of the QNAP device, user accounts, and applications. Out of the box, QNE Network provides built-in features that allow you to easily configure cloud and network settings. QNE Network also comes with the Application Store, which offers various applications for customizing the device and optimizing task workflows.

QNE Network supports two operating modes that can address different business needs. Stand-Alone Mode allows you to manage each QNE Network device separately using local accounts. Meanwhile, Cloud Management Mode allows you to remotely deploy and manage all devices in your organization using AMIZ Cloud, a central cloud management platform for QNAP devices.

QNE Initialization

QNE provides two operating modes: Stand-alone Mode and Cloud Management Mode. During QNE initialization, you can choose a mode that best meets your needs. You can also switch modes after the initialization.

Initializing QNE Using Stand-alone Mode

Stand-alone Mode is useful for managing a single local device. In this mode, you must manage the device with local accounts, but you can remotely access the device using the myQNAPcloud service.

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

1. Power on the device.
2. Connect the device to your local area network.
3. Run Qfinder Pro on a computer that is connected to the same local area network.

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

4. Locate the device in the list and double-click the name or IP address.
   The **Smart Installation Guide** opens in the default web browser.
5. Perform any of the following actions.
   - To install the out-of-the-box version, click **Next**.
   - To check for the latest available version, click **Check for Update**, and then click **Update**. The device restarts after the wizard downloads the latest available version. If a newer version is unavailable, the wizard automatically displays the **Smart Installation Guide**.

- To manually specify a version, click **Browse**, select a file, and then click **Update**.

6. Click **Start** under Stand-alone Mode.

Tip
QNAP recommends enabling auto-update for software components. This ensures that your system stays up to date.

7. Specify the following information.
   - **Host name**: Specify a name with 1 to 15 characters. The name supports letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), but cannot end with a hyphen.
   - **Username**: Specify a name with 1 to 32 characters. The name supports letters (A to Z, a to z), numbers (0 to 9), and hyphens (-), but cannot end with a hyphen.
   - **Password**: Specify an administrator password with 1 to 64 characters. The password supports all ASCII characters.
   - **Confirm password**: Enter your password again.
8. Click **Next**.
9. Review application disk information.

Important
QNE stores the data of virtual machines and containers on application disks. If you have already installed disks on the device, QNE automatically configures disks and chooses an appropriate RAID type based on the number of disks. If you have not installed disks, QNAP recommends shutting down the device after the initialization and then installing disks.

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

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

12. Click **Apply**.
    QNE is installed.

Installing QNE Using Cloud Management Mode

Cloud Management Mode is ideal for organizations that have multiple remote devices. You can access centrally deploy and manage your devices in AMIZ Cloud and access them with your QNAP ID.

To deploy your device in this mode, you need to create an AMIZ Cloud join key and send the join key to the device administrator. For details, visit https://amizcloud.qnap.com and see Adding a Device Using an AMIZ Cloud Join Key.

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

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

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

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

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

5. Perform any of the following actions.

   - To install the out-of-the-box version, click **Next**.
   - To check for the latest available version, click **Check for Update**, and then click **Update**. The device restarts after the wizard downloads the latest available version. If a newer version is not available, the wizard automatically displays the **Smart Installation Guide**.
   - To manually specify a version, click **Browse**, select a file, and then click **Update**.

6. Click **Start** under Cloud Management Mode.

7. Review application disk information.

Important
QNE stores the data of virtual machines and containers on application disks. If you have already installed disks on the device, QNE automatically configures disks and chooses an appropriate RAID type based on the number of disks. If you have not installed disks, QNAP recommends shutting down the device after the initialization and then installing disks.

8. Click **Next**.

9. Enter your AMIZ Cloud Join Key.

10. Click **Next**.
AMIZ Cloud installs QNE on your device.

Note
You need to complete the initial device setup in AMIZ Cloud to deploy the device.

Device Access

Method	Description	Requirements
Web browser	You can access the QuCPE device using any computer on the same network if you have the following information: • Device name or IP address (as the URL) For example, http://myDeviceName or http://172.17.50.123 • Login credentials of a valid user account.	• Computer that is connected to the same network as the QuCPE device • Web browser

Method	Description	Requirements
Qfinder Pro	Qfinder Pro is a desktop utility that enables you to locate and access QuCPE devices on a specific network. It supports Windows, macOS, Linux, and Chrome OS.	• Computer that is connected to the same network as the QuCPE device • Web browser • Qfinder Pro
AMIZ Cloud	You can access the QuCPE device from AMIZ Cloud if your QNE is in Cloud Management Mode.	• Internet connection • Web browser

Accessing the QuCPE Device Using a Browser

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

Tip
If you do not know the IP address of the device, you can locate it using Qfinder Pro.
For details, see Accessing the QuCPE Device Using Qfinder Pro.

The QNE login screen appears.

4. Specify your username and password.
5. Click **Login**.
The QNE desktop appears.

Accessing the QuCPE Device Using Qfinder Pro

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

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

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

Accessing the QuCPE Device Using AMIZ Cloud

You can access the QuCPE device from AMIZ Cloud if QNE is in Cloud Management Mode. For details on AMIZ Cloud, see AMIZ Cloud.

1. Go to https://amizcloud.qnap.com/.
2. Sign in with your QNAP ID.

3. Select **Devices**.
   AMIZ Cloud displays a list of devices in your organization.
4. Hover over the device that you want to access.
5. Click .

Tip
You can also select a device and then click beside the device name.

AMIZ Cloud directs you to the selected QuCPE device and opens QNE in a new tab.

QNE Navigation

Desktop

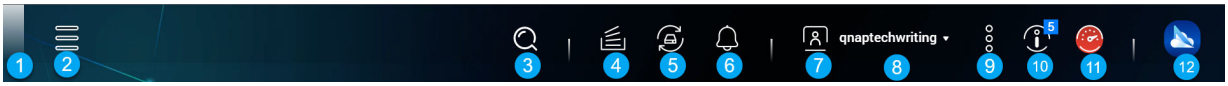
#	Element	Description	Possible User Actions
1	Desktop	This area contains open system utilities and applications. The desktop consists of three separate screens.	• Click **<** or **>** to move to another desktop. • Change the QNE desktop wallpaper in the **Options** window by selecting one of the built-in options or uploading an image. For details, see Options.

#	Element	Description	Possible User Actions

2	Shortcut icons	Each icon opens an app or a utility. After installing an application, QNE automatically creates a desktop shortcut.	• Click an icon to open the application window.
			• Right-click an icon and then select one of the following:
			  • **Open**: Opens the application window
			  • **Remove**: Deletes the icon from the desktop
			• Click and drag an icon to another desktop.

3	Date and time	This displays the date and time that the user configured during system installation.	N/A
4	Notifications	This notifies the user about important system events that may require user action. If there are multiple notification groups, notices are arranged according to the notification type on a notice board. You can also view notifications in **Notice Board**.	Click a notification to open the corresponding utility or app.
5	Link bar	This displays shortcut links to myQNAPcloud, utility and app download pages, feedback channels, and the Helpdesk.	Click any of the following buttons: • : Opens the myQNAPcloud website in a new browser tab • : Opens the download page for mobile applications and utilities • : Provides links to the QNAP Wiki, QNAP Forum, and Customer Service portal • : Opens the Helpdesk utility

Task Bar



No.	Element	Possible User Actions
1	**Show Desktop**	Click the button to minimize or restore all open windows.
2	**Main Menu**	Click the button to open the **Main Menu** panel on the left side of the desktop.

No.	Element	Possible User Actions
3	**Search**	**1.** Type keywords to locate settings, applications, and help content. **2.** Click an entry in the search results to open the application, system utility, or **Help Center** window. If the application is not yet installed, QNE opens the corresponding download screen in the **Application Store** window.

4	**Background Tasks**	• Hover over the button to see the number of ongoing background tasks. Examples of background tasks include file backup and multimedia conversion.
		• Click the button to see the following details for each background task:
		  • Task name
		  • Task description
		  • Progress (percentage of completion)
		• Click ◉ to stop a task.

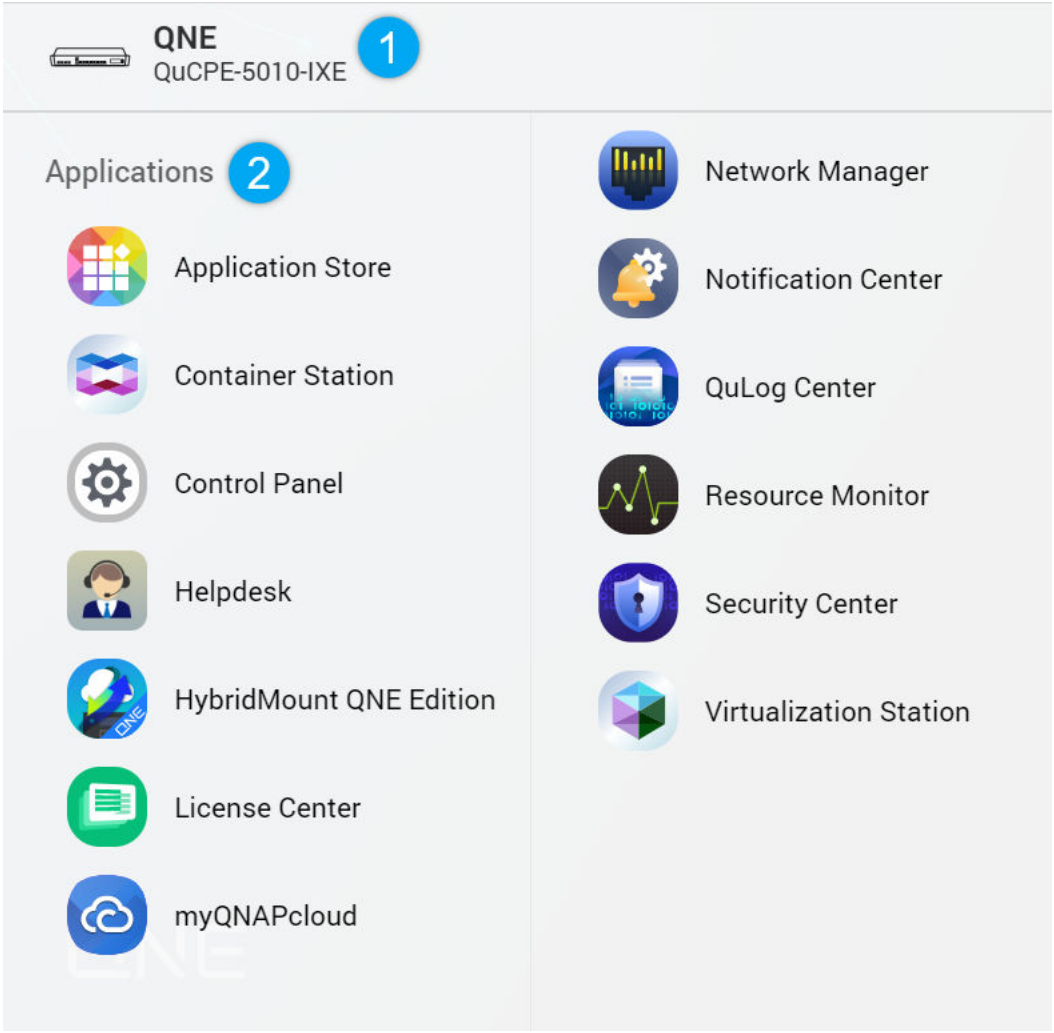
5	**External Devices**	• Hover over the button to view the number of external devices that are connected to the QNE device. • Click the button to view the details for each connected device.

6	**Event Notifications**	• Hover over the button to see the number of recent errors and warnings.
		• Click the button to view the following details for each event:
		  • Event type
		  • Description
		  • Timestamp
		  • Number of instances
		• Click a list entry to view the related utility or application screen. Clicking a warning or error log entry opens the **Event Log** window.
		• Click **More>>** to open **QuLog Center**.
		• Click **Clear All** to delete all list entries.
		Tip
		You can create notification rules in Notification Center.

7	**Options**	Click the profile picture to open the **Options** screen. For details, see Options.

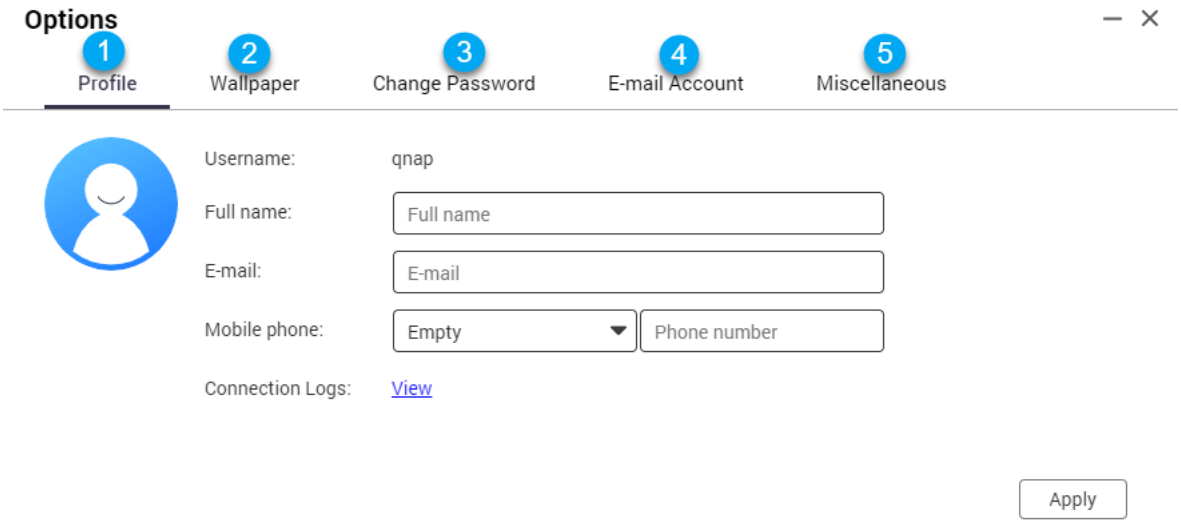
No.	Element	Possible User Actions
8	**[USER_NAME]**	Click the button to view the last login time and the following menu items: • **Options**: Opens the **Options** window For details, see Options. • **Locate This Device**: Sounds the audio alert so you can easily locate the device • **Restart**: Restarts the QNE device • **Shutdown**: Shuts down QNE and then powers off the device **Tip** You can also power off the QNE device using any of the following methods: • Press and hold the power button for 1.5 seconds. • Open Qfinder Pro, locate the device in the list. Right click on the device and select **Shut down Device**. • **Logout**: Logs the user out of the current session
9	**More**	Click the button to view the following menu items: • **Help**: Opens the QNE Web Help page in a new browser tab. • **Language**: Opens a list of supported languages and allows you to change the language of the operating system • **Desktop Preferences**: Opens a list of display modes and allows you to select the mode based on your device type • **Customer Service**: Opens the **QNAP Customer Service** page • **Data & Privacy**: Opens the **QNAP Privacy Policy** page • **About**: Displays the following information: • Operating system • Hardware model • Operating system version
10	**Notice Board**	Display all system notifications and the Getting Started Guide for system setup.
11	**Dashboard**	Click the button to display the dashboard. For details, see Dashboard.
12	**AMIZ Cloud Portal** or **myQNAPcloud**	• In Cloud Management mode, this opens the **AMIZ Cloud Portal** website, where you can centrally deploy, monitor, and manage all your registered devices in the cloud. • In Stand-alone mode, this opens the **myQNAPcloud** website, where you can remotely access your registered devices via the internet.

Main Menu



No.	Section	Description
1	Device Information	Displays the QNE device name and model number.
2	Applications	Displays a list of applications developed by QNAP or third-party developers. When an app is installed, it is automatically added to the applications list.

Options



Note
Some of the following settings are only available in Stand-alone mode.

#	Tab	Possible User Actions

1	**Profile**	• Specify the following optional information:
		  • Profile picture
		  • Full name
		  • E-mail
		  • Mobile phone
		• Click **View** to display the **QuLog Center** screen.
		• Click **Apply** to save all changes.

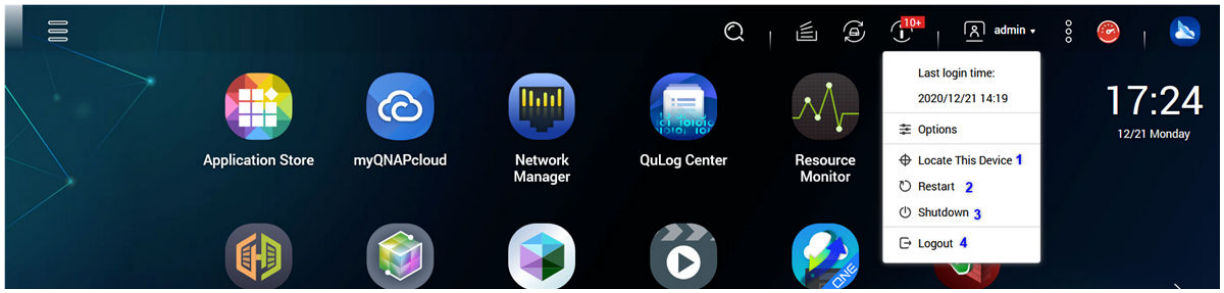
2	**Wallpaper**	• Select a wallpaper from the built-in options or upload a photo. • Click **Apply** to save all changes.

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

#	Tab	Possible User Actions
4	**E-mail Account**	• Add, edit, and delete email accounts that you intend to use when sharing files. • Set an email address as the default account for sharing files. • Click **Apply** to save all changes.

5	**Miscellaneous**	• Enable the following settings.
		  • **Keep me logged in**: When enabled, the current user session stays logged in until the setting is changed.
		  • **Warn me before closing the browser tab**: When enabled, QNE prompts users for confirmation whenever they try to leave the desktop by clicking the **Back** button or closing the browser. QNAP recommends enabling this setting.
		  • **Restore previously open windows when logging in**: When enabled, the current desktop settings and all open windows are retained until the next session.
		  • **Show the desktop screen navigation buttons**: When enabled, QNE displays the desktop switching buttons **< >** on the left and right sides of the desktop.
		  • **Show the Links bar on the desktop**: When enabled, QNE displays the link bar at the bottom of the desktop.
		  • **Show the Dashboard button on the Task bar**: When enabled, QNE displays the Dashboard button on the task bar.
		  • **Show the system time on the desktop**: When enabled, QNE displays the system time and date on the desktop.
		• Click **Apply** to save all changes.

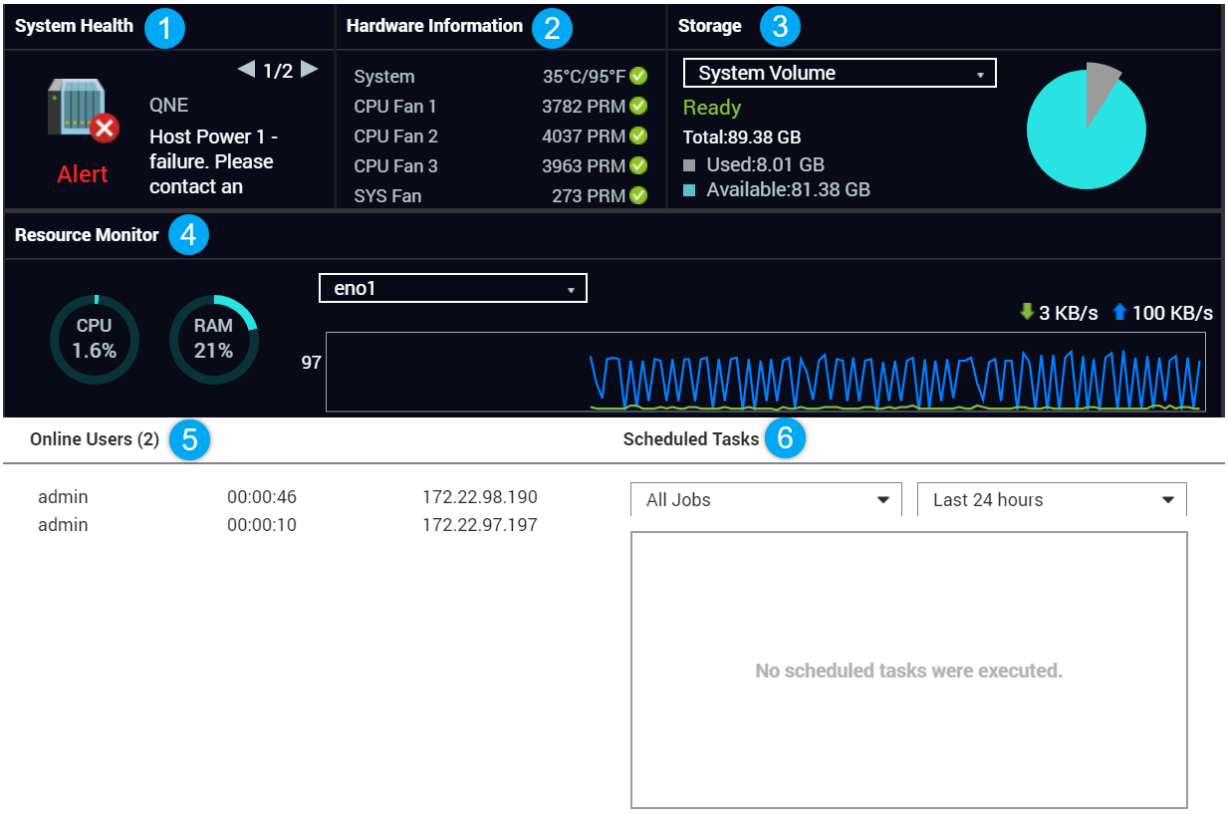
Basic Operations



The basic operations drop-down menu appears when you click next to the profile icon. The following table lists the basic operations that you can perform.

No.	Options	User Actions
1	**Locate This Device**	**1.** Click **Locate This Device**. The **Locate This Device** window appears. **2.** Select the audio alert duration. **3.** Select one or more signal types. **4.** Click **Start**.
2	**Restart**	Click **Restart**. The device is restarted.
3	**Shutdown**	Click **Shutdown**. The device is shut down.
4	**Logout**	Click **Logout**. The user is logged out of the device.

Dashboard



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

Tip
You can click and drag a section to any area on the desktop.

#	Section	Displayed Information	User Actions
1	System Health	• QNE device name • Uptime (number of days, hours, minutes and seconds) • Health status	Click the heading to open the **System Information** screen in the **System Status** window.
2	Hardware Information	• System temperature • CPU fan speed • System fan speed	Click the heading to open the **Hardware Information** screen in the **System Status** window.
3	Storage	For each volume: • Status • Total space • Used space • Available space	Click the heading to open the **Storage Resource** screen in the **Resource Monitor** window. Click ▼ to switch between the following volume types: **System Volume**, **System Data Volume**, and **Application Volume**.
4	Resource Monitor	• CPU usage in % • Memory usage in % • Network upload and download speeds/rates	Click the heading to open the **Overview** screen in the **Resource Monitor** window.
5	Online Users	• Username • Session duration • IP address	Click the heading to open the **QuLog Center** window. You can click **Online Users** to review information on any users currently connected to the device.
6	Scheduled Tasks	• Task type • Task summary • Task name • Timestamp • Status	Use the filters to view tasks that were executed within a specific period.

Getting Started

QNE provides both Stand-alone and Cloud Management modes to meet your needs. You can select a mode during QNE initialization and switch modes after the initialization. The initial setup process may vary depending on which mode you select.

1. Access QNE.

Mode	User Action
Stand-Alone Mode	If you select Stand-Alone Mode during QNE initialization, you can access the device using the administrator account. You can create more local accounts for other users. For details, see User Accounts. You can also create a QNAP ID and register your device to myQNAPcloud to remotely access this device when needed. For details, see myQNAPcloud.
Cloud Management Mode	If you select Cloud Management Mode during QNE installation, you have registered the device to your existing QNAP ID and your organization. You can access QNE using your QNAP ID and centrally manage your devices on AMIZ Cloud. For details, see AMIZ Cloud.

2. Configure system settings.
   For details, see System Settings.
3. Configure network settings.
   For details, see Network Manager.
4. Install applications and utilities.
   For details, see Application Store.
5. Optional: Mount shared folders with HybridMount QNE Edition.
   For details, see HybridMount.

2. Control Panel

The Control Panel allows you to view and configure various settings, including system settings, user accounts, shared folders, and service settings.

System Settings

System Settings allows you to configure the following settings:

- General settings
- Hardware settings
- Power settings
- System update settings
- Backup and restore settings
- Uninterruptible power supply
- System status

General Settings

Settings	Description
System Administration	This screen allows you to specify the server name and ports and configure secure connection settings.
Time	Time settings affect event logs and scheduled tasks. This screen allows you to specify the time zone and format and configure the system date and time.
Daylight Saving Time (DST)	Daylight saving time (DST) settings apply only to regions that use DST. This screen allows you to either automatically adjust the system clock or manually configure the settings.
Region	This screen allows you to select a region for your device. System and application content and services are localized according to the selected region.

Configuring System Administration Settings

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

Field	User Action
Host name	Specify a name containing up to 15 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Dashes (-) **Important** • The host name must contain one or more letters. • The host name cannot consist of numbers only. • The host name cannot start with a dash.
System port	Specify the port used to access the web interface. The default port is 80. **Important** Configuring a blocked port or port reserved for other services is not allowed.
myQNAPcloud device name	Shows the name of the myQNAPcloud device. **Note** This field only appears when myQNAPcloud is enabled.
Enable HTTP compression	Select this option to improve transfer speeds and bandwidth utilization. This setting is enabled by default. **Warning** Enabling this option may lead to security risks.
Enable secure connection (HTTPS)	Select this option to allow users to connect to the device using HTTPS. **a.** Select **Enable secure connection (HTTPS)**. **b.** Select a TLS version. The default TLS version is 1.2. **Warning** Selecting the latest TLS version may decrease compatibility for other clients in your system. **c.** Specify a port number. **d.** Optional: Select **Force secure connection (HTTPS) only** to require all users to connect to the device using only HTTPS.

Field	User Action
Disallow QNE embedding in IFrames	**a.** Select this option to prevent websites from embedding QNE using IFrames. **b.** Optional: Click **Allowed Websites** to allow specific websites to embed QNE in IFrames. The **Allowed Websites** window appears. **c.** Optional: Click **Add** to add a website to the list. The **Add Host Name** window appears. **d.** Specify a host name. **e.** Click **Add**. The host name is added to the allowed websites list. **f.** Optional: Select a website, and then click **Delete** to delete a website from the list. **g.** Click **Apply**.

3. Click **Apply**.

Configuring Time Settings

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

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

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

Option	User Action
Manual setting	Specify the date and time.
Synchronize with a time server automatically	Ensure that your device is connected to the internet, and then specify the following information: • **Server**: Name of the Network Time Protocol (NTP) server Examples: time.nist.gov, time.windows.com • **Time interval**: Number of hours or days between each time synchronization task

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

5. Click **Apply**.

Configuring Daylight Saving Time

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

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

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

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

Configuring Region Settings

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

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

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

Region	Description
China	Select this region if the device is located in China.

3. Click **Apply**.

Disk Information

Screen	Description
Disk Information	This screen allows you to monitor general disk information.
SMART Information	This screen allows you to monitor the SMART disk information.
Test	This screen allows you to test the disk for errors. 1. Select a disk. 2. Select **Test**. 3. Select a test method. 4. Click **Test**.
Settings	This screen allows you to set optional temperature alarms and SMART test schedules. • Select a disk. • Select **Settings**. • Optional: Click **Enable temperature alarm** and specify the temperature and unit. • Optional: Click **Enable rapid test** and then specify the frequency and time. • Optional: Click **Enable complete test** and then specify the frequency and time. • Click **Apply to Selected Disks** to apply the settings to the selected disk, or click **Apply to All Disks** to apply the settings to all disks.

Hardware

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

Note
SR-IOV settings only appears if the hardware supports it.

Configuring General Hardware Settings

1. Go to **Control Panel** > **System** > **Hardware** > **General** .
2. Select **Enable configuration reset switch**.
3. Optional: Enable the system reserved account.

Note
You can use the system reserved account "system-maintainer" to log in to the device for maintenance purposes.

a. Press and hold the reset button on the device for 3 seconds.
The system reserved account is enabled.

4. Optional: Disable the system reserved account.

Note
This option is only available if you enabled the system reserved account.

a. Click **Disable this account**.
A confirmation message appears.

b. Click **OK**.
The system reserved account is disabled.

5. Click **Apply**.

Configuring Audio Alert Settings

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

Setting	Description
System operations	Select to trigger an audio alert every time the device starts, shuts down, or upgrades firmware.
System events	Select to trigger an audio alert when errors or warnings occur.
Disk operations	Select to trigger an audio alert when degrade mode or RAID sync events occur.

3. Click **Apply**.

Configuring Smart Fan Settings

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

Setting	User Action
Enable Smart Fan (recommended)	Select from the two automatic fan speed adjustment options. **a.** The device monitors the temperatures of the system, disks, and CPU and automatically adjusts the fan speed. **b.** The device adjusts the fan speed according to user-specified temperatures. **Note** Modes are only available for system fans. • **Quiet mode**: Fans run on low speed to decrease noise. • **Normal mode**: Fans run on normal speed. This is the default setting. • **Performance mode**: Fans run on high speed to lower the system temperature. This mode is suitable for high loading systems.
Set fan rotation speed manually	Move the slider to set the fan speed.

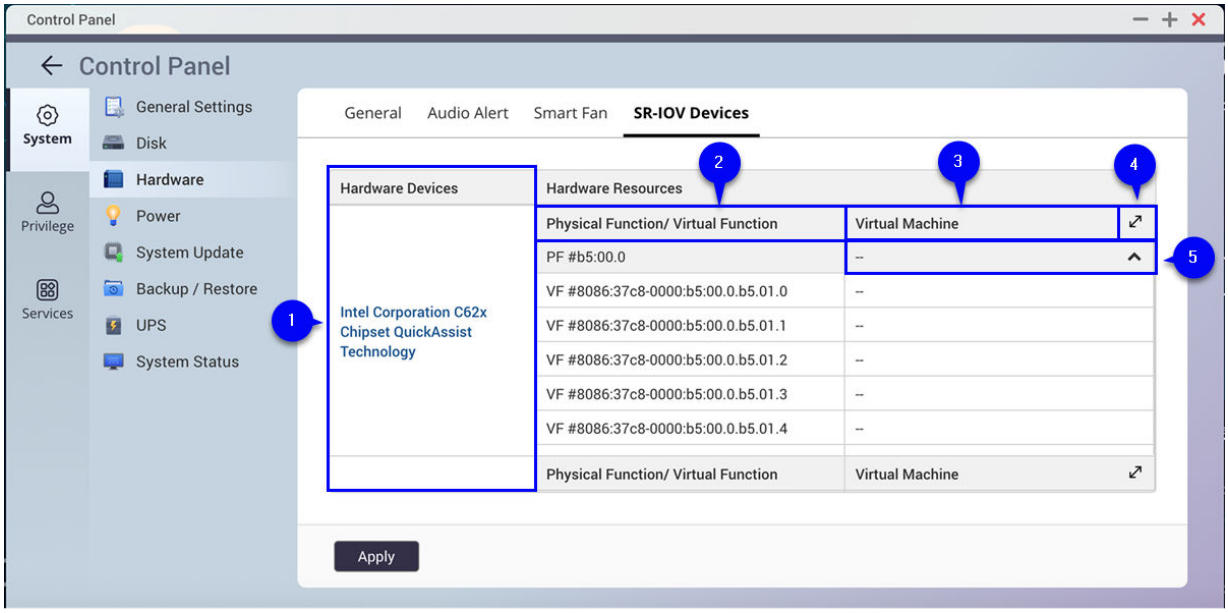
3. Click **Apply**.

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

Note
SR-IOV settings only appears if the hardware supports it.

You can view all Single Root I/O Virtualization (SR-IOV) devices mapped to your virtual machines on the **Control Panel** > **Hardware** > **SR-IOV Devices** page. The SR-IOV interface is a hardware specification that allows a single PCIe device, such as a network adapter, to appear as multiple physical devices to the hypervisor. Because each device is directly assigned to an instance, it can bypass the hypervisor and virtual switch layer to achieve low latency and performance matching nonvirtualized environments. SR-IOV achieves this through the following types of functions:

- Physical Function (PF): These are PCIe devices that have SR-IOV capabilities. PFs are managed and configured in the same way as PCIe devices.
- Virtual Function (VF): These are lightweight PCIe functions that only process I/O. Because each VF is derived from a PF, the device hardware limits the number of VFs a device can have. A VF shares one or more hardware resources of the device, such as a memory or network port.
  The following table lists all SR-IOV functions you can view in **SR-IOV Devices**:



No.	Settings	Description
1	Hardware Devices	Lists all the SR-IOV devices that are mapped to your virtual machine (VM).
2	Physical Function/Virtual Function	Displays the physical function (PF) or virtual function (VF) configured to the SR-IOV device.
3	Virtual Machine	Shows the virtual machines that are mapped to the PF or VF.
4	Resize	Click ⤢ to enlarge or minimize the SR-IOV device panel window.
5	Show or Hide	Click ^ to show or hide the list of SR-IOV device details.

For details on how to configure an SR-IOV device to a VM, see the Virtualization Station user guide.

Power

Settings	Description
Power Recovery	This screen allows you to configure whether the device restarts after a power outage.
Power Schedule	This screen allows you to schedule the system to automatically power on, power off, or restart at specified times.

Configuring Power Recovery

1. Go to **Control Panel** > **System** > **Power** > **Power Recovery** .
2. Configure the power recovery settings.
   a. Click **Power Recovery**.
   b. Select a power recovery setting.
   c. Click **Apply**.

Configuring the Power Schedule

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

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

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

System Update

QNAP recommends keeping your operating system version up to date. This ensures that your device can benefit from new features, enhancements, and bug fixes.

Firmware Update

You can check for QNE device firmware updates on the Firmware Update page. You can also click **Digital Signature** to view the digital signature details of the current firmware version.

Firmware Update Requirements

Your device must meet the following requirements to perform a firmware update:

Settings	Requirements
Hardware settings	• A computer **Important** A computer is required when updating the firmware manually or using Qfinder Pro. • Ethernet cables **Important** QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection remains stable during the firmware update process.
System reboot	QNAP recommends rebooting the device system before the firmware update.
Administrator privileges	You must be a device administrator or have admin privileges to update firmware.
Stop device operations	QNAP recommends stopping all other device operations before the firmware update. The device must restart before the firmware update takes effect and this may disrupt ongoing device services or operations.
Device model name	Ensure you have the correct device model name. You can find the device model name using the following methods: • Locate the model name on a sticker on the bottom or rear of your device. • Go to **Control Panel** > **System Status** > **System Information** > **Model name**
Firmware version	If you are updating the firmware manually or using Qfinder Pro, ensure the selected firmware version is correct for your device model.

Checking for Firmware Updates

1. Go to **Control Panel** > **System** > **System Update** > **Firmware Update** .
2. Click **Check for Update**.
   The system checks for available firmware updates. You can choose to update the operating system if there is an available update.
3. Optional: Click **Automatically check if a newer version is available when logging into QNE**.

Tip
You can view the firmware update status in **Background Tasks**.

4. Click **Apply**.

Updating the Firmware Manually

Warning

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

Important

- Read the Firmware Update Requirements before updating the firmware.
- The update may require several minutes or longer, depending on your hardware configuration and network connection.

1. Download the device firmware.
   a. Go to https://www.qnap.com/download.
   b. Select your device model.
   c. Read the release notes and confirm the following:
      - The device model matches the firmware version.
      - Updating the firmware is necessary.
      - Check for any additional firmware update setup instructions.
   d. Ensure that the product model and firmware are correct.
   e. Select the download server based on your location.
   f. Download the firmware package.
   g. Click **Browse**.
   h. Select a folder.
   i. Save the downloaded firmware package.
2. Go to **Control Panel** > **System** > **System Update** > **Firmware Update** .
3. Click **Browse** and then select the extracted firmware package file.
4. Click **Update System**.
   A confirmation message window appears.

Important
If no further action is taken, the firmware update will automatically start within 60 seconds.

5. Click **OK**.
   The device is immediately restarted.

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

Updating the Firmware Using Qfinder Pro

Warning

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

Important

- Make sure you read through the Firmware Update Requirements before updating QNE.
- The update may require several minutes or longer, depending on your hardware configuration and network connection. Do not power off the device during the update.

1. Download the device firmware.
   a. Go to https://www.qnap.com/download.
   b. Select your device model.
   c. Read the release notes and confirm the following:
      - The device model matches the firmware version.
      - Updating the firmware is necessary.
      - Check for any additional firmware update setup instructions.
   d. Ensure that the product model and firmware version are correct.
   e. Download the firmware package.
2. Open Qfinder Pro.
   Qfinder Pro displays a list of devices on your network.
3. Select a device model from the list.
4. Right click the device model on the list and then select **Update Firmware** .
   The **Firmware Update** window appears.
5. Specify your QNE username and password.
   To update the firmware, you must be the administrator of the selected device.
   Qfinder Pro displays the **Update Firmware** screen.
6. Select one of the following firmware update methods:

Methods	Steps
Update firmware manually	a. Click **Path of firmware package file**. b. Click **Browse**. c. Locate the downloaded firmware package file. d. Click **OK**.
Update firmware automatically	a. Click **Automatically update the firmware to the latest version**. b. Qfinder Pro searches for the latest firmware update.

7. Click **Start**.

Software Component

You can check for QNE device software component updates on the **Software Component** page. You can go to the **Action** column to enable, disable, and update software components.

Configuring a Software Component

1. Go to **Control Panel** > **System** > **System Update** > **Software Component** .
2. Select a software component.
3. Go to the **Actions** column.
4. Select one of the following options:

Options	User Actions
Enable	Click **Start**.
Disable	Click **Stop**.
Remove	Click **Remove**.
Update	Click **Update**.

Checking for Software Component Updates

1. Go to **Control Panel** > **System** > **System Update** > **Software Component** .
2. Click **Check for Update**.
   The system checks for available system updates.

Updating the Software Component

1. Go to **Control Panel** > **System** > **System Update** > **Software Component** .
2. Select one of the following options.

Option	User Action
Update all software components	**a.** Click **Update All**. **b.** Click **OK**.
Update individual software components	**a.** Locate the software component. **b.** Click **Upgrade**. **Note** The **Upgrade** button appears only when a new version is available.

Configuring an Update Schedule

1. Go to **Control Panel** > **System** > **System Update** > **Software Component** .
2. Click **Schedule Setting**.
   The **Schedule Setting** window appears.
3. Click **Install all updates automatically**.
4. Specify the frequency and time.
5. Click **OK**.

Backup/Restore

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

Backing Up System Settings

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

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

Restoring System Settings

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

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

System Reset and Restore to Factory Default

The system provides several options for resetting or restoring the device to its default state.

Important
QNAP recommends backing up your data before performing this task.

Option	Description	Steps
Reinitialize the device	This deletes all data on the disks and reinstalls the operating system.	1. Go to **Control Panel** > **System** > **Backup/Restore** > **Restore to Factory Default** . 2. Click **Reinitialize Device**. 3. Choose to restart or shut down the device after the device is reinitialized. 4. Click **OK**.

Uninterruptible Power Supply (UPS)

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

You can check the UPS information in **Control Panel** > **System** > **UPS** .

You can view the AC power status, battery capacity, estimated protection time, UPS manufacturer, and model on the **UPS Information** page.

Configuring UPS Settings

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

Mode	User Actions
USB connection	**a.** Connect the UPS to the device using a USB cable. **b.** Select **USB connection**. **c.** Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the device to enter auto-protection mode after the power fails for a specified time period **Note** In auto-protection mode, the device stops all services and unmounts all volumes to protect your data. After the power is restored, the device restarts and resumes normal operation. **d.** (Optional) Select **Enable network UPS master** and then specify the IP addresses to which QNE sends notifications in the event of power failure. **Note** This option can only be selected when the UPS is connected to the device via USB.
SNMP connection	**a.** Connect the UPS to the same network as the device. **b.** Select **SNMP connection**. **c.** Specify the IP address of the UPS. **d.** Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the device to enter auto-protection mode after the power fails for a specified time period

Mode	User Actions
Network standby UPS	**a.** Connect the UPS to the same network as the device. **b.** Select **Network UPS slave**. **c.** Specify the IP address of the UPS server. **d.** Choose one of the following options. • Power off the server after the power fails for a specified time period • Allow the device to enter auto-protection mode after the power fails for a specified time period

3. Click **Apply**.

Device Behavior During a Power Outage

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

Phase	Scenario	Network Device
Phase 1: From the start of the power outage until the end of the specified waiting time	The power outage occurs.	The device detects the remaining UPS power.
	The UPS power is greater than 15%.	Depending on your UPS settings, the network device powers off or switches to auto-protection mode after the specified waiting time elapses.
	The UPS power is less than 15%.	Depending on your UPS settings, the device powers off or switches to auto-protection mode after the specified waiting time elapses.
	The power is restored.	The device remains functional.
Phase 2: From the end of the specified waiting time until the UPS runs out of power	The power is not restored, and the device is in auto-protection mode.	The device stops all running services.
	The power is not restored, and the device is powered off.	The device remains powered off.
	The power is restored, and the device is in auto-protection mode.	The device remains powered off.
	The power is restored, and the device is powered off.	The device remains powered off.
Phase 3: From the moment the UPS runs out power until the power is restored	The power is not restored, and the device is in auto-protection mode.	The device powers off.
	The power is not restored, and the device is powered off.	The device remains powered off.
	The power is restored.	The device applies the specified power recovery settings.

System Status

You can check the status of your device in **Control Panel** > **System** > **System Status** .

Section	Description
System Information	This screen displays basic system information, including the server name, model name, CPU, Intel QuickAssist Technology (Intel QAT) support, serial number, BIOS version, memory, dual-channel memory support, firmware version, system up time, time zone, and filename encoding.
Network Status	This screen displays the current network settings of each network interface.
Hardware Information	This screen displays the device hardware information, such as CPU usage, memory, disk temperature, power supply unit (PSU) status, and system fan speed.

User Accounts

All accounts can perform the same actions as an administrator account. They can access all applications and create a shared folder.

Creating a User Account

1. Go to **Control Panel** > **Privilege** > **Users** .
2. Click **Create**.
   The **Create a User** window appears.
3. Specify the following information.

Field	Description
Profile photo	Optional: Upload a profile photo for the user.
User Description (optional)	Specify a user description that contains a maximum of 50 characters.
Username	Specify a username that contains 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Dashes (-)
Full name	Optional: Specify the full name of the user.
Password	Specify a password that contains a maximum of 64 ASCII characters.
Verify Password	Enter the password again.

Field	Description
Mobile Phone	Specify a phone number that will receive SMS notifications from this device. For details, see SMS Notifications. **Note** Other users might be able to see this information. If you do not want to share this information, leave the field blank.
Email (optional)	Specify an email address that will receive notifications from this device. For details, see Email Notifications. **Note** Other users might be able to see this information. If you do not want to share this information, leave the field blank.
Send a notification mail to the newly created user (optional)	When selected, this device sends a message to the specified email address that contains the following information: • Username and password • URLs for connecting to this device **Tip** You can edit the notification message.

4. Click **Create**.

Modifying User Account Information

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

Task	User Action
Change password	**a.** Under **Action**, click . The **Change Password** window appears. **b.** Specify a password that contains up to 64 ASCII characters. **c.** Verify the password. **d.** Click **Apply**.

Task	User Action
Edit account profile	**a.** Under **Action**, click . The **Edit Account Profile** window appears. **b.** Modify any of the following fields: • **Full name** • **Email** • **Mobile phone** • **Description (optional)** **c.** Optional: Disable the account. 1. Select **Disable this account**. 2. Select when to disable the account. • **Now**: The account will be disabled after clicking **OK**. • **Expiry date**: The account will be disabled on the specified date. **d.** Click **OK**.

Deleting User Accounts

1. Go to **Control Panel** > **Privilege** > **Users** .
2. Select the user accounts you want to delete.

Note
The administrator account cannot be deleted.

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

Shared Folders

To create a shared folder, you must install HybridMount. For details on installing HybridMount, see Installing HybridMount. Shared folders are considered as a remote mount. For more information on remote mounts, see Remote Mounts.

Creating Shared Folders

This task explains how to create a shared folder from the Control Panel. You can also create a shared folder directly from HybridMount.

1. Go to **Control Panel** > **Privilege** > **Shared Folders** .
2. Click **Create**.
   HybridMount opens.

Tip
To mount a cloud service, see Mounting a Cloud Service Using File Cloud Gateway. To mount a remote device, see Mounting a Remote Device.

Editing Shared Folders

This task explains how to edit a shared folder from the Control Panel. You can also edit a shared folder directly from HybridMount.

1. Go to **Control Panel** > **Privilege** > **Shared Folders** .
2. Locate the shared folder you want to edit and click .
   The **Edit Mount** window opens.

Tip
To edit a cloud mount, see the edit connection settings option in Managing a Cloud Service Mount. To manage a remote mount, see the edit connection settings option in Managing a Remote Device Mount.

Enabling File Protocols and File Station Access to Shared Folders

Depending on your environment, you may want to enable a different file protocol for your shared folders to access remote data. You can also hide your shared folders on File Station.

1. Go to **Control Panel** > **Privilege** > **Shared Folders** .
2. Identify the shared folder or cloud service and select at least one of the following.

Note
Depending on the original file protocol, your shared folders may be subject to protocol restrictions. A FTP or WebDAV shared folder can only support their own file protocols.

Option	Description
Samba	Enables the SMB file protocol. **Note** A shared folder mounted using the FTP or WebDAV file protocol cannot support this option.
FTP	Enables the FTP file protocol. **Note** A shared folder mounted using the WebDAV file protocol cannot support this option.
NFS	Enables the NFS file protocol. **Note** A shared folder mounted using the FTP or WebDAV file protocol cannot support this option.
WebDAV	Enables the WebDAV file protocol. **Note** A shared folder mounted using the FTP file protocol cannot support this option.

Option	Description
File Station	Shows or hides the shared folder on File Station. **Note** Hiding the shared folder on File Station does not unmount the shared folder.

Tip

- To create a shared folder, click **Create** at the top-left corner.
- To edit a mount, click under the **Action** column.

3. Click **Apply**.

Service Settings

The following system services are provided.

Note
If any service is disabled or removed, the application disappears from the Control Panel.

Service	Description
SSH	Secure Shell (SSH) is a network protocol used for securely accessing network services over an unsecured network. Enabling SSH allows users to connect to the NAS using an SSH-encrypted connection or a SSH client such as PuTTY. **Note** You can disable and remove the SSH Server from the Application Store.
SNMP	The Simple Network Management Protocol (SNMP) is used to collect and organize information about managed devices on a network. Enabling the SNMP service allows for the immediate reporting of device events, such as warnings or errors, to a Network Management Station (NMS). **Note** You can disable and remove the SNMP Service from the Application Store.

Service	Description
Service Discovery	You can enable the following services: • Universal Plug and Play (UPnP) Discovery Service: UPnP is a networking technology that enables the discovery of networked devices connected to the same network. After enabling this service, devices supporting UPnP can discover the this device. **Note** The UPnP Service is not available on the Application Store. • Bonjour: Bonjour is a networking technology developed by Apple that enable devices on the same local area network to discover and communicate with each other. **Note** The Bonjour Service is not available on the Application Store.
NTP	The Network Time Protocol (NTP) is a networking protocol for synchronizing clocks between computer systems to Coordinated Universal Time (UTC). **Note** • The NTP Server is disabled by default. • You can disable and remove the NTP Server from the Application Store.
Samba	Samba is a Microsoft networking protocol that allows data to be accessed over a computer network and provides file and print services to Windows clients. **Note** You can disable and remove the Samba Server from the Application Store.
FTP	The File Transfer Protocol (FTP) is a standard network protocol for transferring files between servers and clients on computer networks. **Note** You can disable and remove the FTP Server from the Application Store.
NFS	The Network File System (NFS) is a file system protocol that allows data to be accessed over a computer network. Enabling the NFS service allows Linux and FreeBSD users to connect to the device. **Note** You can disable and remove NFS server from the Application Store.

Service	Description
WebDAV	The Web Distributed Authoring and Versioning (WebDAV) is an extension of HTTP that allows clients to perform remote web content authoring operations. **Note** You can disable and remove the WebDAV Server from the Application Store.

Configuring SSH Connections

Important
Only administrator accounts can access the device through SSH.

1. Go to **Control Panel** > **Services** > **SSH Server** .
2. Select **Allow SSH connection**.
3. Specify a port number.
   Port numbers range from 1 to 65535.

Tip
The default SSH port is 22.

4. Click **Apply**.

Configuring SNMP Settings

1. Go to **Control Panel** > **Services** > **SNMP Service** .
2. Select **Enable SNMP Service**.
3. Configure the SNMP settings.

Setting	User Action
Port number	Specify the port that the Network Management Station (NMS) will use to connect to this device.
SNMP Trap Level	Select the type of alert messages that this device will send to the NMS.
Trap Address	Specify the IP addresses of the NMS. You can specify a maximum of 3 trap addresses.

4. Select the SNMP version that the NMS uses.

Option	User Action
SNMP V1/V2	Specify an SNMP community name that contains 1 to 64 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and this device. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.
SNMP 3	Specify the username, authentication protocol and password, and privacy protocol and password. **a.** Specify a username. **Note** The username should contain 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ **b.** Optional: Select **Use Authentication**. **1.** Specify the authentication protocol. **Tip** You can select either **HMAC-MD5** or **HMAC-SHA**. If you are unsure about this setting, QNAP recommends selecting **HMAC-SHA**. **2.** Specify an authentication password that contains 8 to 64 ASCII characters. **c.** Optional: Select **Use Privacy**. **1.** Specify a privacy password that contains 8 to 64 ASCII characters.

5. Click **Apply**.

Downloading the SNMP MIB

1. Go to **Control Panel** > **Services** > **SNMP Service** .
2. Under **SNMP MIB**, click **Download**.
   This device downloads the device MIB file to your computer.

Enabling the UPnP Discovery Service

1. Go to **Control Panel** > **Services** > **Service Discovery** > **UPnP Discovery Service** .
2. Select **Enable UPnP Discovery Service**.
3. Click **Apply**.

Configuring Bonjour Settings

1. Go to **Control Panel** > **Services** > **Service Discovery** > **Bonjour** .
2. Select **Enable Bonjour Service**.
3. Select the services to be advertised by Bonjour.

Important
You must enable the services in this device before advertising them with Bonjour.

4. Click **Apply**.

Configuring NTP Server Settings

1. Go to **Control Panel** > **Services** > **NTP Server** .
2. Select **Enable NTP Server**.
3. Optional: Select one or more operating modes.
   - **Broadcast**: Data is transported from one source to all possible destinations.
   - **Multicast**: Data is transported from one source to multiple destinations that state interest in receiving the data.
     This mode requires you to enter an IP address.
   - **Manycast**: Data is transported between multiple sources and destinations.
     This mode requires you to enter an IP address.
4. Click **Apply**.

Configuring Microsoft Networking

1. Go to **Control Panel** > **Services** > **Samba Server** .
2. Select **Enable file service for Microsoft networking**.
3. Configure Microsoft networking settings.

Setting	User Action
Server description (Optional)	Specify a description that contains a maximum of 256 characters. The description must enable users to easily identify this device on a Microsoft network.

Setting	User Action
Workgroup	Specify a workgroup name that contains 1 to 15 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: ~ ! @ # $ ^ & ( ) - _ { } . '

4. Optional: Configure any of the following settings.

Option	User Action
Enable WINS server	Select this option to run a WINS server on this device.
Use the specified WINS server	Select this option to specify a WINS server IP address that this device will use for name resolution. Do not select this option if you are unsure about the settings.
Enable local master browser	Select this option to use this device as a local master browser. A local master browser is responsible for maintaining the list of devices in a specific workgroup on a Microsoft network. When deselected, another device on the network maintains the device list. **Important** To use the this device as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".
Allow only NTLMSSP authentication	Select this option to authenticate clients using only NT LAN Manager Security Support Provider. When this option is deselected, this device uses NT LAN Manager (NTLM).
Name resolve priority	Select a name service to use for name resolution. The default service is **DNS only**. If a WINS server is specified, **Try WINS then DNS** is selected by default.
Enable Asynchronous I/O	Select this option to improve the Samba performance using asynchronous I/O. Asynchronous I/O refers to the I/O behavior on the CIFS protocol layer. This is different from the synchronous I/O feature found in the shared folder settings, which only applies to specific shared folders on the file system level. **Tip** To prevent power interruption, use a UPS when asynchronous I/O is enabled.

Option	User Action
Highest SMB version	Select the highest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting. **Note** Selecting SMB3 will also include SMB3.1 and SMB3.1.1.
Lowest SMB version	Select the lowest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting. **Note** Selecting SMB3 will also include SMB3.1 and SMB3.1.1.
Lock File (Oplocks)	Opportunistic lock (Oplocks) is a Windows file locking mechanism that facilitates caching and access control to improve performance. This feature is enabled by default and should only be disabled in networks where multiple users simultaneously access the same files.
Only allows applications to access files using the long file name format	When selected, applications can only use the long file name (LFN) format to access files.

5. Click **Apply**.

Configuring FTP Settings

1. Go to **Control Panel** > **Services** > **FTP Server** .
2. Select **Enable FTP Service**.
3. Configure the followings settings.

Setting	User Action
Protocol type	Select at least one FTP type.
Port	Specify a port number between 1 and 65535.
Enable anonymous	Select this option to allow anonymous users to access files via FTP.
Maximum number of all FTP connections	Specify a value between 2 and 1024.
Maximum number of connections for a single account	Specify a value between 2 and 1024.
Maximum upload rate (KB/s)	Select this option to specify the maximum upload rate of files over FTP. You must specify a value of at least 1.
Maximum download rate (KB/s)	Select this option to specify the maximum upload rate of files over FTP. You must specify a value of at least 1. **Note** The maximum number of allowed connections for a single account must be lower than the maximum number of total allowed FTP connections.
Passive FTP port range	Specify a passive FTP port range between 1025 and 65535. The default range is 55536-56559.

4. Click **Apply**.

Configuring NFS Settings

1. Go to **Control Panel** > **Services** > **NFS Server** .
2. Select one of the following options.
   - **Enable NFS v2/v3 Service**
   - **Enable NFS v4 Service**
3. Optional: Add or remove allowed IP addresses or domains.

Action	Steps
Add an IP address or domain	**a.** Under **Allow IP Address or Domain Name**, click **Add**. A new field appears in the table. **b.** Specify the IP address or domain.
Remove an IP address or domain	**a.** Under **Allow IP Address or Domain Name**, locate the IP address or domain you want to remove. **b.** Select the IP address or domain. **c.** Click **Remove**.

4. Click **Apply**.

Configuring WebDAV Settings

1. Go to **Control Panel** > **Services** > **WebDAV Server** .
2. Click **Enable WebDAV**.
   a. Optional: Click **HTTP port number**.
   b. Optional: Specify a port number between 1 and 65535.
   c. Optional: Click **HTTPS port number**.
   d. Optional: Specify a port number between 1 and 65535. This number may not be the same as Http port number.

3. Storage Space

Storage Space allows administrators to monitor information on system disks and volumes.

Disks

QNE uses a system boot disk for the system volume and system data volume, and optionally one or more application disks for the application volume. For details, see Volumes.

To view general information on a disk, go to **Storage Space** > **Disk** , select a disk, and then select **Disk Information**.

To view S.M.A.R.T. information on a disk, go to **Storage Space** > **Disk** , select a disk, and then select **SMART Information**.

You can also perform S.M.A.R.T. tests on disks, and configure S.M.A.R.T. test schedules and disk temperature alarms.

Running a S.M.A.R.T. Test on a Disk

1. Open Storage Space.
2. Go to **Disk**.
3. Select a disk.
4. Go to **Test**.
5. Select a test method.

Test Method	Description
Rapid test	Tests the electrical and mechanical properties of the disk, and a small portion of the disk surface. This test generally completes within one minute.
Complete test	Tests the electrical and mechanical properties of the disk, and the full disk surface. The test duration depends on the storage environment.

6. Click **Test**.

QNE runs a S.M.A.R.T. test on the selected disk.

Configuring a S.M.A.R.T. Test Schedule

1. Open Storage Space.
2. Go to **Disk**.
3. Select a disk.
4. Go to **Setting**.
5. Optional: Select **Enable rapid test**.

Note
A rapid test tests the electrical and mechanical properties of the disk, and a small portion of the disk surface. This test generally completes within one minute.

a. Select a schedule.

Schedule	Description
Daily	Runs the test once every day.
Weekly	Runs the test once every week. Specify a day of the week.
Monthly	Runs the test once every month. Specify a day of the month.

b. Specify a time to run the test.

6. Optional: Select **Enable complete test**.

Note
A complete test tests the electrical and mechanical properties of the disk, and the full disk surface. The test duration depends on the storage environment.

a. Select a schedule.

Schedule	Description
Daily	Runs the test once every day.
Weekly	Runs the test once every week. Specify a day of the week.
Monthly	Runs the test once every month. Specify a day of the month.

b. Specify a time to run the test.

7. Click **Apply to Selected Disks** to apply the settings to the selected disk, or click **Apply to All Disks** to apply the settings to all disks.

QNE applies the S.M.A.R.T. test schedule settings.

Configuring a Disk Temperature Alarm

1. Open Storage Space.
2. Select **Disk**.
3. Select a disk.
4. Select **Setting**.
5. Select **Enable temperature alarm**.
6. Specify a temperature threshold.

Note
The system issues a warning when the disk temperature exceeds the specified threshold.

7. Click **Apply to Selected Disks** to apply the settings to the selected disk, or click **Apply to All Disks** to apply the settings to all disks.

QNE applies the disk temperature alarm settings.

Volumes

There are three types of volumes on QNE: system volume, system data volume, and application volume.

To view information on a volume, go to **Storage Space** > **Volume** and select a volume.

System Volume

The system volume stores the operating system, including system libraries and utilities.

This volume is created on the system boot disk.

System Data Volume

The system data volume stores system configuration files and databases.

This volume is created on the system boot disk.

Application Volume

The application volume stores virtual machine and container applications.

After the system initializes or starts, a RAID group is created from the application disks, and then the application volume is created on the RAID group.

4. Network Manager

Network Manager is a QNE utility that centralizes the creation, configuration, and control of network connections. Network Manager also manages physical network interfaces, WAN and LAN settings, and port trunking in addition to controlling DHCP, DDNS, and gateway services.

Configuring Network Settings

This section describes how to configure the network settings in Network Manager, including the physical network settings, traffic mapping settings, and virtual network settings.

Configuring Network and IP Addressing Settings

This section describes how to configure WAN, LAN, DDNS, DHCP, port trunking, and RADVD settings.

Configuring WAN Port Settings

1. Open Network Manager.
2. Go to **WAN** > **WAN Ports** .
3. Identify a port to configure.
4. Click  .
   The **WAN Configuration** window appears.
5. Configure the WAN IP settings.

Setting	User Action
Obtain IP address settings automatically via DHCP	Select this option to automatically obtain an IP address. If the network supports DHCP, the device automatically obtains the IP address and network settings.

Setting	User Action
Static IP	Select this option to manually specify an IP address. Manually assign a static IP address. You must specify the following information: • Fixed IP address • Subnet mask • Default gateway • DNS server 1 Select **Use static IPv6** address to use IPv6 instead of IPv4. When selected, you must specify the following information: • Fixed IP address • Prefix length **Tip** Obtain the prefix length information from your network administrator. • Default gateway **Important** • The prefix must be between FE80 and FEBF. • The IPv6 default gateway IP address must be from the same subnet as the fixed IP address.
PPPoE	Select this option to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

6. Configure the remaining settings.

Setting	User Action
ISP line rate	Specify the gross bit rate of the physical layer.
Metric	Specify the number of nodes that the route will pass through. **Note** Metrics are cost values used by routers to determine the best path to a destination network.

Setting	User Action
Jumbo frames	Specify the size of the Jumbo Frames. Jumbo frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QNE supports the following MTU sizes: • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes **Important** • All connected network devices must enable Jumbo Frames and use the same MTU size. • Using jumbo frames requires a network speed of 1000 Mbps or faster.

7. Click **Apply**.

Network Manager updates the WAN port settings.

Configuring LAN Port Settings

1. Open Network Manager.
2. Go to **LAN** > **LAN Ports** .
3. Identify a port to configure.

Note
A port must first be assigned to the LAN. For details, see Configuring Physical Port Settings.

4. Click .
The **LAN Configuration** window appears.
5. Configure LAN IP settings.

Setting	User Action
Fixed IP address	Specify a fixed IP address. **Tip** Examine your network setup for guidance on how to best configure these settings.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.

Setting	User Action
Use static IPv6 address	Select this option to use IPv6 instead of IPv4. When selected, you must specify the following information: • Fixed IP address • Prefix length **Tip** Obtain the prefix length information from your network administrator.

6. Configure network interface controller (NIC) settings.

Setting	User Action
Jumbo frames	Specify the size of the Jumbo Frames. Jumbo frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QNE supports the following MTU sizes: • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes **Important** • All connected network devices must enable Jumbo Frames and use the same MTU size. • Using jumbo frames requires a network speed of 1000 Mbps or faster.
Network Speed	Select the network transfer rate allowed by the network environment. **Tip** Selecting **Auto-negotiation** will automatically detect and set the transfer rate. **Important** The Network Speed field is automatically set to **Auto-negotiation** and hidden when configuring 10GbE & 40GbE adapters.

7. Click **Apply**.

Network Manager configures the settings.

Adding and Configuring a DDNS Server

1. Open Network Manager.
2. Go to **WAN** > **DDNS** .

3. Click **Add DDNS**.
   The **Add DDNS** window appears.

4. Configure the DDNS settings.

Setting	User Action
WAN port	Specify the WAN port for the DDNS server.
DDNS server	Select the DDNS service provider. **Note** When selecting **Customized**, you must specify the **Profile name**.
Username	Specify the username for the DDNS service.
Password	Specify the password for the DDNS service.
Hostname	Specify the hostname or domain name for the DDNS service.
Automatic external IP check interval	Specify how often to update the DDNS record.

5. Click **Apply**.

Network Manager adds the DDNS server.

Creating and Configuring a Trunking Group

1. Open Network Manager.
2. Go to **LAN** > **Port Trunking (LACP)** .
3. Click **Go to Port Trunking Configuration**.
   The **Port Trunking Configuration** window appears.
4. Select two or more ports to add to the trunking group.
5. Select a hash policy.
6. Click **Save**.

Network Manager creates the trunking group.

Creating and Configuring a DHCP Server

This screen controls the creation and management of DHCP servers. DHCP servers can assign IPv4 addresses to clients on the network, while RADVD servers assign IPv6 addresses.

Important
Do not create a new DHCP server if one already exists on the network. Enabling multiple DHCP servers on the same network can cause IP address conflicts or network access errors.

1. Open Network Manager.
2. Go to **LAN** > **DHCP Server** > **DHCP Server** .
3. Click **Add DHCP Server**.
   The **DHCP Server** window appears.

4. Configure the settings.

Setting	User Action
Port	Select a port.
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server. **Note** QNAP recommends specifying at least one DNS server to allow URL lookups.

5. Optional: Specify additional settings.

   a. Click **More Settings**.
   Additional DHCP settings appear.

   b. Configure the settings.

Setting	User Action
WINS Server	Specify the WINS server IP address. **Tip** Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix. **Tip** The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server. **Tip** QNE supports both PXE and remote booting of devices.
Boot File	Specify location and file name of the TFTP server boot file. **Tip** QNE supports both PXE and remote booting of devices.

6. Click **Apply**.

Network Manager creates the DHCP server.

Creating and Configuring an RADVD Server

The Router Advertisement Daemon (RADVD) sends messages required for IPv6 stateless auto-configuration. It also sends router advertisement (RA) messages periodically to the LAN.

1. Open Network Manager.
2. Go to **LAN** > **DHCP Server** > **RADVD** .
3. Click **Add RADVD**.
   The **Add RADVD** window appears.
4. Configure the settings.

Setting	User Action
WAN port	Select a WAN port for outgoing connections.
RA service port	Select a LAN port to connect to the server.
Prefix	Specify the prefix for the IP address.
Prefix Length	Specify the prefix length for the adapter. **Tip** Obtain the prefix and the prefix length information from your ISP.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server. **Note** QNAP recommends specifying at least one DNS server to allow URL lookups.

5. Click **Apply**.

Network Manager creates the RADVD server.

Configuring NCSI Settings

1. Open Network Manager.
2. Go to **WAN** > **NCSI** .
3. Identify a port to configure.
4. Configure the NCSI settings.

Setting	User Action
NCSI Service	Enable or disable the Network Connectivity Status Indicator (NCSI) service. **Tip** The NCSI periodically performs tests to check the speed and status of network connections.

Setting	User Action
Checking Method	Select the checking method for the NCSI service: • **QNAP**: The WAN port pings ncsi.qnap.com to check the network connection. • **Default gateway**: The WAN port pings the port's default gateway to check the network connection. • **Custom address**: The WAN port pings the specified domain or IP address to check the connection. This option requires you to specify a domain name or IP address.

5. Click **Apply**.

Network Manager updates the NCSI settings.

Configuring Physical Port Settings

1. Open Network Manager.
2. Go to **Advanced Settings** > **Physical Port Definition** .
3. Identify a port to configure.
4. Modify the port definition.

Definition	User Action
WAN	Select to use the port for wide area networks (WANs).
LAN	Select to use the port for local area networks (LANs).
VNF	Select to use the port for virtual network functions (VNFs).

Important
The port definition cannot be modified when a DHCP server, port trunking, VLAN, or RADVD is enabled.

5. Click **Apply**.

Network Manager updates the physical port settings.

Configuring Port Routing and Mapping

This section describes how to configure static route and port mapping settings on Network Manager.

Creating IPv4 and IPv6 Static Routes

This section controls the creation of static routes. Under normal circumstances, QNE automatically obtains routing information after it has been configured for Internet access. Static routes are only required in special circumstances, such as having multiple IP subnets located on your network.

1. Open Network Manager.
2. Go to **Advanced Settings** > **Static Route** > **Static Route** .
3. Under **Type**, select the IP version.

4. Click **Add Static Route**.
   The **Static Route** window appears.

5. Configure the settings.

Setting	User Action
Destination	Specify a static IP address where connections are routed to.
Metric	Specify the number of nodes that the route will pass through. **Note** Metrics are cost values used by routers to determine the best path to a destination network.
Port	Select the interface that connections should be routed through.
IPv4 Static Route	
Netmask	Select the destination prefix length for the IPv6 static route.
Gateway	Specify the IP address of the destination's gateway.
IPv6 Static Route	
Prefix length	Specify the prefix length for the adapter. **Tip** Obtain the prefix and the prefix length information from your ISP.
Next hop	Specify the IP address of the closest or most optimal router in the routing path.

6. Click **Apply**.

Network Manager creates the static route.

Tip
To delete a static route, select the static route type, select the static route checkbox and click **Delete**.

Adding a 1:1 Network Address Translation (NAT) Rule

1. Open Network Manager.
2. Go to **Advanced Settings** > **1:1 NAT & Port Forwarding** .
3. Click **Add Rule**.
   The **Add Rule** window appears.
4. Configure the rule settings.

Setting	User Action
Port	Select a port.
Type	Select **1:1 NAT**.
LAN IP	Specify the LAN IP address.

Setting	User Action
Allowed remote IPs	Specify one or more remote IP addresses. **Note** Leaving this field blank allows access from any remote IP address.
Description	Enter a description for the rule.

5. Click **Apply**.

Network Manager adds the rule.

Adding and Configuring a Port Forwarding Rule

1. Open Network Manager.
2. Go to **Advanced Settings** > **1:1 NAT & Port Forwarding** .
3. Click **Add Rule**.
   The **Add Rule** window appears.
4. Configure the rule settings.

Setting	User Action
Port	Select a port.
Type	Select **Port forwarding**.
WAN service port	Specify the type of WAN service for the rule.
LAN IP	Specify the LAN IP address.
LAN service port	This field displays LAN service port information.
Allowed remote IPs	Specify one or more remote IP addresses. **Note** Leaving this field blank allows access from any remote IP address.
Description	Enter a description for the rule.

5. Click **Apply**.

Network Manager adds the port forwarding rule.

Configuring Virtual Network Settings

This section describes how to configure the virtual network settings in Network Manager.

Adding and Configuring a VLAN

1. Open Network Manager.
2. Go to **LAN** > **VLAN** .
3. Click **Add VLAN**.
   The **Add VLAN** window appears.
4. Configure the VLAN settings.

Setting	User Action
LAN interface	Select a port or trunking group as the LAN interface.
VLAN ID	Specify a VLAN ID. **Important** • The VLAN ID must be between 1 and 4094. • Make a note of the VLAN ID before completing this process. If the VLAN ID is lost, the network settings will need to be reset.
Description	Enter a description between 1 and 32 characters.
Fixed IP address	Specify a fixed IP address. **Tip** Examine your network setup for guidance on how to best configure these settings.
Subnet mask	Specify the subnet mask used to subdivide your IP address.
Use static IPv6 address	Select this option to use IPv6 instead of IPv4. When selected, you must specify the following information: • Fixed IP address • Prefix length **Tip** Obtain the prefix length information from your network administrator.

5. Click **Apply**.

Network Manager adds the VLAN.

Enabling OVS-DPDK on Native Ports

The Open Virtual Switch with Data Plane Development Kit (OVS-DPDK) is an open source distributed, multilayer virtual switch that enables fast packet forwarding by enabling DPDK. You can enable OVS-DPDK to accelerate quick network function virtualization (NFV) deployment.

1. Open Network Manager.
2. Go to **Advanced Settings** > **Network CPU Management** > **OVS-DPDK** .
3. Select **Enable OVS-DPDK**.

Important
You must restart to finalize this step.

4. Select the CPU socket from the drop-down list.

Note
This setting is available only on models that support multiple CPU sockets.

5. Select a CPU allocation method.

Method	Description
Shared	Allows you to share CPU cores with other applications and services.
Dedicated	Allows you to dedicate CPU cores to the native port. Dedicated cores are not available to external NIC ports.

6. Select the required number of CPU cores.
7. Click **Apply**.
   Network Manager applies the changes.
8. Restart the QNE device.
9. Open Network Manager.
10. Go to **Advanced Settings** > **Network CPU Management** > **Enabled Ports** .
11. Assign the VNF ports to the native port.
12. Click **Apply**.

Network Manager enables OVS-DPDK acceleration on the selected native ports.

Allocating CPU Resources

This section describes how to allocate shared and dedicated CPU resources on your device using Network Manager.

1. Open Network Manager.
2. Go to **Advanced Settings** > **Network CPU Management** > **Physical Ports** .
3. Identify a native port.
4. Click  .
   The **Allocate CPU Resources** window opens.
5. Select a CPU allocation method.

Method	Description
Shared	Allows you to share CPU cores with other applications and services.
Dedicated	Allows you to dedicate CPU cores to the native port. Dedicated cores are not available to external NIC ports.

6. Select the CPU socket from the drop-down list.

Note
This setting is available only on models that support multiple CPU sockets.

7. Select the required number of CPU cores and threads.

Note

- You can allocate only two threads for native port CPU resources.
- You cannot select CPU cores reserved for system operations.

8. Click **Save**.

Network Manager allocates the CPU resources to the native port.

Monitoring Network Settings

This section describes how to access and monitor network operations in Network Manager.

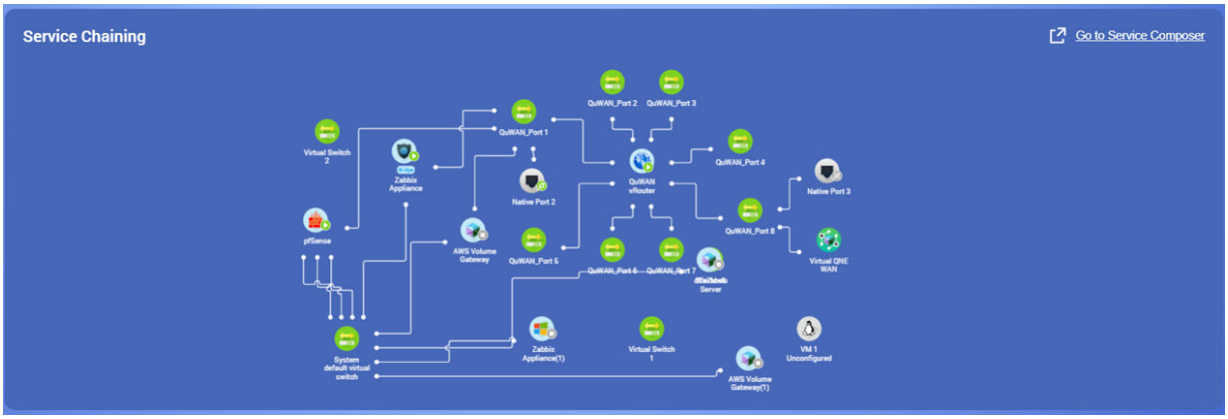
Viewing Port Configurations

1. Open Network Manager.
   The **Overview** page opens and displays the following information:

Item	User Action
	Click to view the WAN settings enabled on the native port. View the following information: • Current WAN IP address • Primary DNS server • Secondary DNS server
	Click to view the LAN settings enabled on the native port. View the following information: • Current LAN IP address • VLAN ID
	Click to view ports enabled with virtual network functions.
Navigation	
	Click to navigate forward on the overview section.
	Click to navigate back on the overview section.

Viewing Service Chaining Configurations

1. Open Network Manager.
   Service chaining information is displayed on the **Overview** page.



2. To configure service chaining, click **Go to Service Composer**.

Service Composer application opens.

Deleting Network Settings

This section describes how to delete network settings in Network Manager.

1. Open Network Manager.
2. Identify a network setting.
3. Click .
   A confirmation message appears.
4. Click **Delete**.

Network Manager deletes the network setting.

5. Service Composer

About Service Composer

Service Composer allows you to assign and provision physical and virtual network elements to create and manage services in a virtual environment. You can map these services to different composite applications, such as SD-WAN, security, and servers. With Service Composer you can simplify complex services or create new services using virtual components.

Installation and Navigation

This section describes how to install Service Composer on your device and how to navigate through the various elements of the application.

System Requirements

Service Composer is available in Application Store.

Category	Requirements
Hardware	A compatible QNAP device.
Software	• QNE 1.0.2 or later • Virtualization Station For details, see Virtualization Station and Virtualization Station System Requirements.

Installing Service Composer

1. Go to Application Store.
2. Enter Service Composer in the search bar.
   The Service Composer app installation package appears.
3. Download Service Composer.
4. Click **Install**.

QNE installs Service Composer.

Service Composer Elements

This section illustrates the various Service Composer elements that you can use to configure composite applications.

Tool Icon	Tool Description	Description
Toolbar		

Tool Icon	Tool Description	Description

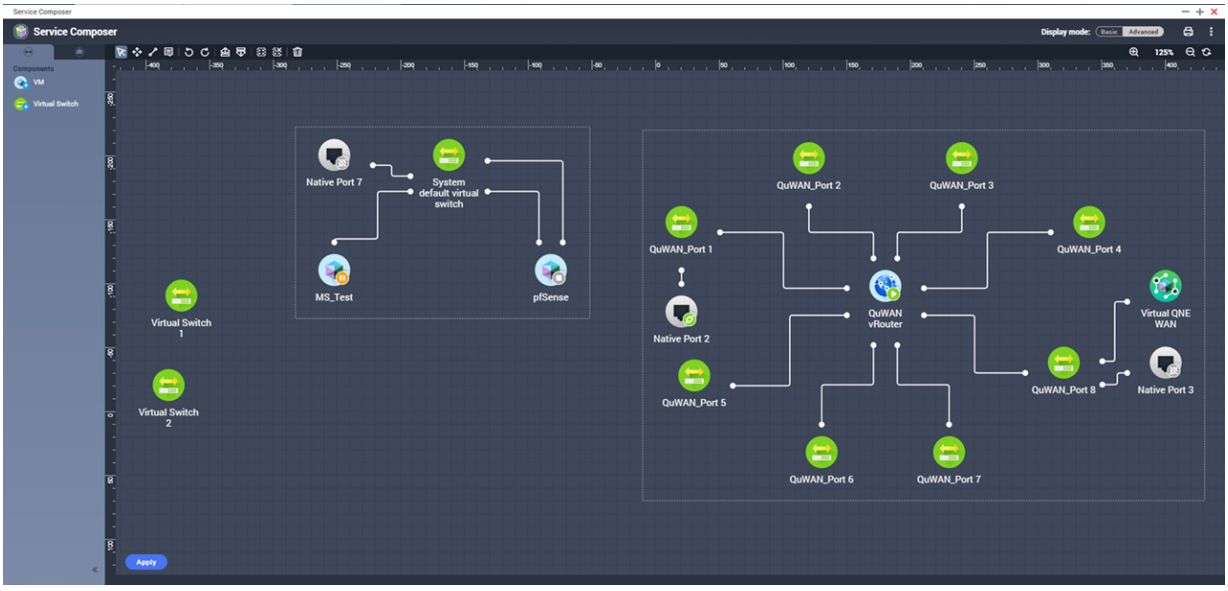
	Cursor	Performs the following functions:
		• Selects and drags individual components on to the canvas
		• Displays the following VM options when you right-click the cursor:
		  • Start
		  • Suspend
		  • Shutdown
		  • Force shutdown
		• Highlights service connectors

	Move	Drags the canvas within the Service Composer application
	Service connector	Connects two service components by adding an adapter
	Comment	Adds comments on the canvas
	Undo	Performs the undo function **Note** You cannot undo an action after applying changes to the canvas.
	Redo	Performs the redo function on an undone action
	Bring to Front	Changes the stack layer by bringing a component to the top of the stack
	Send to Back	Changes the stack layer by sending a component to the bottom of the stack
	Group	Groups service components to form a composite application
	Ungroup	Ungroups a grouped composite application
	Delete	Deletes a composite application or a specific service components
	Zoom in	Displays a smaller area of the canvas
	Zoom out	Displays a wider area of the canvas
	Zoom percentage	Displays a smaller or wider area of the canvas
	Refresh	Refreshes the canvas contents

Tool Icon	Tool Description	Description
Basic Advanced	Canvas display mode	Displays the canvas in the following modes: • **Basic**: Displays the basic service connectors in a composite application • **Advanced**: Displays all the service connectors in a composite application
	Print	Prints the current Service Composer canvas
	More	• **Help**: Displays the Help document for more information on Service Composer • **About**: Displays the application information including the version number
Left Panel		
	Software Component	Displays the following software components: • Virtual machine • Virtual Switch • QuWAN vRouter For details, see Adding a Software Component.
	Virtual Network Function (VNF) ports	Displays the list of VNF ports For details, see Adding and Configuring VNF Ports.

Service Composer Canvas

The Service Composer canvas is a graphical tool that enables users to model software components and VNF ports that serve as part of composite applications.



Using Service Composer

This section describes how to add and configure software components and VNF ports to create composite applications through service chaining.

Software Components

The following software components can be added and configured in Service Composer:

Software Component	Description
Virtual Machine	A virtual machine is a software computing resource that uses files named "images" to run software programs and applications in a virtual environment. VMs can be deployed as standalone operating systems or virtual applications.
Virtual Switch	A virtual switch is a virtual network component that allows virtual machines (VMs) to communicate with each other or with networks outside the virtual infrastructure.

VNF Ports

Virtual Network Function (VNF) ports are virtual elements within a network with well-defined external interfaces and network functions such as DHCP, firewall, switches, routers, and WAN optimizers. VNFs can be configured in QNE Network Manager.

Adding Software Components

1. Open Service Composer.
2. Select  .
3. Identify a software component from the list.
4. Click and drag the software component icon on to the canvas.
5. Click **Apply**.

Service Composer adds the software component to the canvas.

Adding and Configuring VNF Ports

This section describes how to configure and add Virtual Network Function (VNF) ports in Service Composer.

1. Open Service Composer.
2. Click  .
   The **Physical VNF Port** page appears.
3. Click **Settings**.
   The Network Manager application opens.
4. Identity a physical port in **Advanced Settings** > **Physical Port Definition** .
5. Under **VNF**, enable the checkbox corresponding to the physical port.
6. Click **Apply**.
   A confirmation message appears.

7. Click **Yes**.
   Network Manager saves the settings.
8. Reopen Service Composer.
9. Identify the native port.
10. Click and drag the icon on to the canvas.
11. Select  .
12. Click the native port icon.
    The connector line appears.
13. Click on a software component.
    Service Composer establishes a service chain between the physical VNF port and the software component.
14. Click **Apply**.

Service Composer saves the settings.

Configuring VM Settings

1. Open Service Composer.
2. Identify a virtual machine or a QuWAN vRouter.
3. Click the VM.
   The **Information** page appears on the right panel.
4. Click **Settings.**
   The Virtualization Station application opens.
5. Configure the settings.
   For details, see the Virtualization Station Help on QNE.
6. Click **Apply**.

Service Composer saves the VM settings.

Configuring Virtual Switch Settings

1. Click the virtual switch.
   The **Information** page appears on the right panel.
2. Click **Settings**.
   The **Virtual Switch** window appears.
3. Select the IP Address Management (IPAM) capability function.

Setting	User Action
Disable IPAM	Select if the virtual switch is connected to a VM that is preconfigured with a DHCP service enabled network segment.
Enable IPAM	Select to enable the IPAM capability on the virtual switch to forward traffic to the connected VNF. Configure the static IPAM settings.

	• **Fixed IP address**: Specify a fixed IP address. • **Subnet mask**: Specify the subnet mask used to subdivide your IP address.

4. Click **Apply**.

Service Composer saves the settings.

Advanced Composite Applications

This section describes how to configure and manage advanced composite service applications using Service Composer components on the canvas. You can compose a service which combines operations specified in several back-end services.

Creating QuWAN vRouter Composite Application

This section describes how to configure a QuWAN vRouter application using Service Composer.

Ensure that your device meets the following minimum requirements before installing QuWAN vRouter:

Resource	Minimum Requirements
CPU threads	• 2 dedicated threads for supported CPU pins (greater than or equal to 4 cores and 8 threads) • 2 shared threads for unsupported CPU pins (less than 4 cores and 8 threads)
Memory	1 GB
Network ports	2 unoccupied ports

Note
The following IP subnets are reserved by QuWAN internal resources:

- 127.0.0.0/8
- 169.254.0.0/16
- 198.18.0.0/15
- 224.0.0.0/8

1. Log in to QNE with your QNAP ID.
2. Configure VNF ports.
   a. Open Network Manager.
   b. Go to **Advanced Settings** > **Physical Port Definition** .
   c. Enable VNF on two native ports.
   d. Click **Apply**.
   A confirmation message appears.
   e. Click **Yes**.
3. Open Service Composer.

4. Click and drag **QuWAN vRouter** onto the canvas.
5. Double-click **QuWAN vRouter Unconfigured**.
6. Click **Start**.
   The **QuWAN vRouter Settings** window appears.
7. Configure the QuWAN_Port 1 settings.
   a. Click ⚙.
      The **QuWAN_Port 1** settings window appears.
   b. Configure the WAN IP settings.

Setting	User Action
Obtain IP address settings automatically via DHCP	Select to automatically obtain an IP address. If the network supports DHCP, the device automatically obtains the IP address and network settings.
Static IP	Select to manually specify an IP address. Manually assign a static IP address. You must specify the following information: • Fixed IP address • Subnet mask • Default gateway
PPPoE	Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).
ISP line rate	Specify the gross bit rate of the physical layer.
Description	Specify a description for the WAN port.

   c. Select a native port.
   d. Enable SR-IOV on the port.

Note
You can enable SR-IOV only if the external network card supports the Single Root I/O Virtualization (SR-IOV) function.

   e. Click **Apply**.
      QuWAN vRouter updates the QuWAN_Port 1 settings.
8. Configure the QuWAN_Port 8 settings.
   a. Click ⚙.
      The **QuWAN_Port 8** settings window appears.
   b. Configure LAN IP settings.

Setting	User Action
Fixed IP address	Specify a fixed IP address.
Subnet mask	Specify the subnet mask used to subdivide your IP address.

9. Configure the DHCP server settings.

Important
Enable DHCP server is enabled by default.
This setting cannot be disabled. QuWAN vRouter automatically obtains the IP address using DHCP to complete the configuration.

Setting	User Action
Start IP address	Specify the starting IP address in a range allocated to DHCP clients.
End IP address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet mask	Specify the subnet mask used to subdivide your IP address.
Lease time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
DNS server	Specify a DNS server for the DHCP server.
Description	Enter a description for the LAN port.

   a. Click **Apply**.

   b. Click **Next**.

   Service Composer starts installing the QuWAN vRouter.

10. Configure the device settings.

Setting	User Action
Region	Select a region. **Note** Click **Add Region** to create a new region in the organization.
Site	Select a site. **Note** Click **Add Site** to create a new site in the organization.
QuWAN device name	Specify a QuWAN name for the device.
Device role	Select from the following: • **Hub** • **Edge**

Important
You cannot change device roles or join a selected region if the regional hub has more than thirty VPN tunnel connections.

11. Click **Next**.
    Service Composer configures the device settings.

12. Click **Finish**.

13. Click **Apply**.

Service Composer saves the QuWAN vRouter settings.

Creating a Virtual Firewall Application

This section describes how to configure a virtual firewall application using service chaining.

1. Create a virtual firewall application.
   a. Open Service Composer.
   b. Click and drag **VM** on to the canvas.
   c. Double-click the unconfigured VM.
      The **Create VM** page appears.
   d. Select **Firewall** as the VM type.
   e. Click **Next**.
   f. Select a VNF mode.

Setting	Description
Router	The VNF behaves as a virtual router and works in isolation from the physical network.
Bridge	The VNF behaves as a repeater and monitors incoming and outgoing traffic from the VM.

   g. Click **Next**.
   h. Under **Category**, select **VNF**.
   i. Select **pfSense**.

Note
You can also install any third-party virtual firewall application while on the **Create VM** page.

   j. Click **Apply**.
      Service Composer installs the virtual firewall application.
   k. Click **Apply**.
      Service Composer saves the virtual firewall application.
2. Configure the virtual firewall settings in Virtualization Station.
   a. Open Virtualization Station.
   b. Under the VM list, identify the pfSense VM.
   c. Click **Settings**.
   d. Configure the VM settings.
      For details, see Installing pfSense on a QNAP Device.

Service Composer saves the settings.

Creating an Anti-Intrusion Composite Application

Service Composer allows you to configure anti-intrusion mechanisms such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to protect your virtual computing and networking resources.

By configuring IDS and IPS virtual machines, you can chain services to secure other composite applications in the system.

1. Create an anti-intrusion application.

   a. Open Service Composer.

   b. Click and drag **VM** on to the canvas.

   c. Double-click the unconfigured VM.
   The **Create VM** page appears.

   d. Select a VM type.

VM Type	Description
IDS	Monitors events on the network and analyzes them for possible security threats.
IPS	Performs security checks and prevents possible security threats to the network.

Note
You can also install any third-party virtual anti-intrusion application while on the **Create VM** page.

   e. Select a VNF mode.

Setting	Description
Router	The VNF behaves as a virtual router and works in isolation from the physical network.
Bridge	The VNF behaves as a repeater and monitors incoming and outgoing traffic from the VM.

   f. Click **Next**.

   g. Under **Category**, select **All Apps**.

   h. Select the VM application.

   i. Click **Apply**.
   Service Composer installs the anti-intrusion application.

   j. Click **Apply**.
   Service Composer saves the anti-intrusion application.

2. Configure the anti-intrusion settings on Virtualization Station.

   a. Open Virtualization Station.

   b. Under the VM list, identify the VM.

   c. Click **Settings**.

   d. Configure the VM settings.
   For details, see the Virtualization Station chapter.

Service Composer saves the settings.

Creating a Guest Operating System

This section describes how to create a guest OS using Service Composer.

1. Open Service Composer.
2. Click and drag **VM** on to the canvas.
3. Double-click the unconfigured VM.
   The **Create VM** page appears.
4. Select an operating system.
5. Click **Next**.
6. Select a VNF mode.

Setting	Description
Router	The VNF behaves as a virtual router and works in isolation from the physical network.
Bridge	The VNF behaves as a repeater and monitors incoming and outgoing traffic from the VM.

7. Click **Next**.
8. Under **Category**, select **Utilities**.
9. Select from the following:
   - **Import VM**
   - **Create VM**
10. Click **Apply**.
    The **Open Virtualization Station** window appears.
11. Click **OK**.
    The Virtualization Station application opens.
12. Configure the guest OS settings on Virtualization Station.
    For details, see the Virtualization Station Help on QNE.

Service Composer saves the settings.

Installing an Ubuntu Linux Operating System

Service Composer allows you to connect to the Ubuntu Linux Station application and helps you install a single Ubuntu Linux operating system.

1. Log on to QNE with your QNAP ID.
2. Open Service Composer.
3. Click and drag Ubuntu Linux Station on to the canvas.
4. Double-click **Ubuntu Linux Station Unconfigured**.
   The **Install Ubuntu Linux Station** window appears.

5. Select the OS version.
6. Click **Install**.

Note
You can only install one version of the Ubuntu Linux operating system.

A notification message appears.

7. Click **OK**.
   A confirmation message appears.
8. Click **OK**.
   Ubuntu Linux Station installs and enables the operating system.
9. Double-click the OS icon.
   The VNC remote desktop viewer opens in a new tab.

Grouping a Composite Application

1. Open Service Composer.
2. Select all the elements of a composite application.
3. Click  .

Service Composer groups the composite application.

Deleting Composite Applications and Software Components

This section describes how to delete a composite application or software component in Service Composer.

Note
Ensure that the composite application or software component is shut down before performing the delete operation.

1. Open Service Composer.
2. Identify a composite application or software component.
3. Select the grouped area or the software component on the canvas.
4. Click  .
   A confirmation message appears.
5. Click **OK**.

Service Composer deletes the composite application or the software component.

6. myQNAPcloud

myQNAPcloud is a service that allows you to access, manage, and share files stored on your QNAP devices remotely through the internet.

Getting Started

1. Create a QNAP ID.
   For details, see Creating a QNAP ID.
2. Select a mode.
   For details, see Mode Selection.
3. Optional: Configure any of the following settings.

Settings	Description
AMIZ Cloud Agent	**Note** This service is only available in the Cloud Management Mode. AMIZ Cloud Agent helps you collect the system analytics of your QNAP device and send the data to AMIZ Cloud. It also allows your device to receive cloud instructions in Cloud Management Mode. This service is enabled by default. For details, see Restoring the AMIZ Cloud Agent Connection.
myQNAPcloud Link	myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote device without needing to first save them to client device. This service is enabled by default.
DDNS	My DDNS allows you to specify a dedicated myQNAPcloud subdomain name that you can use to access your device on the internet. For details, see Configuring DDNS Settings.
SSL certificates	myQNAPcloud allows you to add SSL certificates to help secure your network communication. You can either download and install a myQNAPcloud or Let's Encrypt certificate. For details, see Installing an SSL Certificate.

Account Setup

Before using myQNAPcloud services, you must first create a QNAP ID and then configure required settings using your QNAP ID.

Creating a QNAP ID

QNAP ID allows you to manage your QNAP devices and services. You can create a QNAP ID by using your email address, phone number, or social media account.

Creating a QNAP ID With Email or Phone Number

1. Go to https://account.qnap.com.
   The **QNAP Account** login page displays.
2. Click **Create Account**.
   The **Create Account** screen appears.

3. Specify a nickname, a valid email address or phone number, and a password.
4. Read and acknowledge the Terms of Service and Privacy Policy.
5. Click **Sign Up**.
   The **Data Privacy Notice** box appears.
6. Read the notice, and then click **I Agree**.
   myQNAPcloud sends a verification email or message.
7. Confirm the registration.
   Your QNAP ID is activated.

Tip
The registration link automatically expires in 15 days. You can go to QNAP Account to send a new activation email.

Creating a QNAP ID With Social Media

1. Go to https://account.qnap.com/.
   The **QNAP Account** login page displays.
2. Click **Create Account**.
   The **Create Account** screen appears.
3. Click **Google** or **Facebook**.
   The **Data Privacy Notice** box appears.
4. Read the notice, and then click **I Agree**.
   myQNAPcloud prompts you to log into the selected account.
5. Complete the account creation wizard.
   Your QNAP ID is created.

Creating an Organization

Cloud Management Mode requires you to create an organization in Organization Center.

1. Go to https://organization.qnap.com/.
2. Sign in using your QNAP ID or social media account.
3. Click **Organization**.
4. Click **Create Organization**.
5. Specify the organization information.
   a. Specify the organization name.
   b. Select a country from the list.
   c. Select the approximate number of members in your organization.
   d. Optional: Specify the website URL.
   e. Optional: Specify a contact number.
6. Click **Next**.

7. Optional: Create a group.
   a. Click **Create Groups**.
   b. Specify the group name.
   c. Optional: Add a description.
   d. Click **Create**.
8. Click **Next**.
9. Optional: Invite administrators.
   When you create an organization, you are automatically assigned as an administrator.
   a. Click **Invite Administrators**.
   b. Specify an email address associated with a QNAP ID.
   c. Optional: Select a group.
   d. Optional: Add a description.
   e. Click **Add**.

Tip
You can invite multiple administrators at a time.

   f. Click **Done**.
   myQNAPcloud sends an invitation email or message.

The organization is created and added to the **Organization** dashboard. Administrator can also create sites for different locations of your organization. You can select a site when registering a new device.

Mode Selection

QNE provides two operating modes to address your different business needs. You can choose a mode in myQNAPcloud and switch modes anytime.

Mode	Description
Stand-alone	This mode is useful for managing only the local device. You must log in with local accounts to manage the device. However, you can still remotely access the device using myQNAPcloud service.
Cloud Management	This mode is suitable for organizations with multiple remote devices. Enabling this mode gives administrators access permissions to connected QNAP devices. This allows IT professionals to manage remote devices using AMIZ Cloud, a portal designed for centrally operating, configuring, and monitoring various devices in the cloud. Organization owners and authorized administrators can either log in with their QNAP IDs or with their local accounts.

Enabling Stand-alone Mode

1. Log on to QNE.
2. Open myQNAPcloud.

3. Under **Stand-alone Mode**, click **Get started using a QNAP ID**.
   The **Quick Start for Stand-alone Mode** wizard opens.
4. Specify your QNAP ID and password.
5. Click **Sign In**.
6. Specify a device name containing up to 30 alphanumeric characters.
   You may reuse an existing device name. The device currently using this name will be deregistered from myQNAPcloud.
7. Click **Next**.
8. Enable services.

Service	Description
myQNAPcloud Link	You can configure access controls for myQNAPcloud Link. • **Private**: Only you can find and remotely access your device via myQNAPcloud. • **Public**: Everyone can find your device with your device name and remotely access published services on your device via myQNAPcloud. • **Custom**: Only invited users can find and access your device. If users without permissions try to access your device with a SmartURL, they will not be able to connect to the device.
Server Mode (DDNS)	Dynamic Domain Name Service (DDNS) allows you to automatically map a domain name to the dynamic IP address of your device. With this service, users can connect to your device using the following URL without knowing the current IP address: `[your_device_name].myqnapcloud.com`

9. Click **Apply**.
   Stand-alone Mode is enabled.

Enabling Cloud Management Mode with a QNAP ID

Before enabling Cloud Management Mode with your QNAP ID, you must first create an organization in Organization Center.

Cloud Management Mode allows administrators to manage the device using their QNAP ID instead of local accounts. Note that you must log in with your QNAP ID if you want to make any changes to myQNAPcloud settings in Cloud Management Mode.

1. Log on to QNE.
2. Open myQNAPcloud.
3. Under **Cloud Management Mode**, click **Get started using a QNAP ID**.
   The **Quick Start for Cloud Management Mode** wizard opens.
4. Specify your QNAP ID and password.
5. Click **Sign In**.
6. Select an organization from the list.
   If there are no available organizations, myQNAPcloud prompts you to create one. For details, see Creating an Organization.

7. Select a site from the list.
   If you haven't created any sites, you can select the default site or click **Create**.
8. Click **Next**.
9. Specify a device name containing up to 30 alphanumeric characters.
   You may reuse an existing device name. The device currently using this name will be deregistered from myQNAPcloud.
10. Click **Next**.
    The wizard displays a list of services that are enabled by default.
11. Click **Apply**.
    Cloud Management Mode is enabled.

Enabling Cloud Management Mode with an AMIZ Cloud Join Key

You can generate a join key from AMIZ Cloud and send the key to a device administrator to enable Cloud Management Mode on the device. For details on how to generate a join key, see Adding a Device Using an AMIZ Cloud Join Key.

1. Log on to QNE.
2. Open myQNAPcloud.
3. Under **Cloud Management Mode**, click **Get started using an AMIZ Cloud join key**.
   The **Quick Start for Cloud Management Mode** wizard opens.
4. Specify the join key.
5. Click **Register**.
   The wizard displays a list of services that are enabled by default.
6. Click **Apply**.
   Cloud Management Mode is enabled.

Switching Modes

You can switch between Stand-alone Mode and Cloud Management Mode anytime in myQNAPcloud according to your needs.

Important
AMIZ Cloud only functions in Cloud Management Mode. After you switch from Cloud Management Mode to Stand-alone Mode, all services related to AMIZ Cloud will not be available.

1. Log on to QNE.
2. Open myQNAPcloud.
3. Beside **Mode**, select a different mode from the list.

Mode Switch	User Action
From Cloud Management Mode to Stand-alone Mode	**a.** Select **Stand-alone Mode**. The **Switch to Stand-alone Mode** window appears. **b.** Click **Switch**. The **Quick Start for Stand-alone Mode** wizard appears. **c.** Follow the on-screen instructions to complete the setup. For details, see Enabling Stand-alone Mode.
From Stand-alone Mode to Cloud Management Mode	**a.** Select **Cloud Management Mode**. **b.** Click **Switch**. The **Quick Start for Cloud Management Mode** wizard appears. **c.** Follow the on-screen instructions to complete the setup. For details, see Enabling Cloud Management Mode with a QNAP ID.

Basic Operations and Service Statuses

You can perform basic operations and monitor the status of each myQNAPcloud service on the **Overview** screen. The list of available services varies depending on the selected mode.

Basic Operations

Icon	User Action
	Click to open the AMIZ Cloud Portal. The AMIZ Cloud Portal provides a central management platform for QNAP devices. **Note** This button is only available in Cloud Management Mode.
	• In Cloud Management Mode, click to switch between organizations. The **Quick Start for Cloud Management Mode** wizard appears. Follow the on-screen instructions to complete the configuration. For details, see Enabling Cloud Management Mode with a QNAP ID. • In Stand-alone Mode, click to switch between QNAP IDs. The **Quick Start for Stand-alone Mode** wizard appears. Follow the on-screen instructions to complete the configuration. For details, see Enabling Stand-alone Mode.
	Click to sign out of myQNAPcloud. **Note** If Cloud Management Mode is enabled, you must unregister the device before you can sign in with a different account.
	Click to modify the device name.

Icon	User Action
	Click to copy the SmartURL.

Service Status

Status	Description
Normal	This service is connected to both the internet and the cloud server.
Abnormal	This service is connected to the internet but is unable to connect to the cloud server.
Enabled	This service is enabled and functioning properly.
Disabled	This service is disabled.
Not Installed	This service is not yet installed.

Remote Access Management

myQNAPcloud allows you to configure settings and manage services designed to facilitate remote access and ensure secure connection.

Restoring the AMIZ Cloud Agent Connection

This service is enabled by default. If there are issues with the connection, complete the following steps.

Important
AMIZ Cloud Agent is only available in Cloud Management Mode.

1. Open myQNAPcloud.
2. Go to **AMIZ Cloud Agent**.
3. Click **Reconnect**.

Enabling myQNAPcloud Link

Important
When Cloud Management Mode is enabled, myQNAPcloud Link cannot be disabled.

1. Open myQNAPcloud.
2. Go to **myQNAPcloud Link**.
3. Enable **myQNAPcloud Link**.

Tip
If there are issues with the connection, click **Reconnect**.

Configuring DDNS Settings

myQNAPcloud provides DDNS service to map domain names to dynamic IP addresses. This helps you simply your connection to the device.

Important

If your device is in Cloud Management Mode, you must log in to the device with your QNAP ID in order to make any changes to the settings.

1. Open myQNAPcloud.
2. Go to **DDNS**.
3. Enable **My DDNS**.
4. Perform any of the following tasks.

Task	User Action
Change the myQNAPcloud DDNS domain name	**a.** Click  . The **Change Device Name Wizard** appears. **b.** Specify a device name containing up to 30 alphanumeric characters. **c.** Click **Apply**.
Update myQNAPcloud	Click **Update**.
Manually configure the DDNS IP address	**Note** You can only modify the IP address in Stand-alone Mode. **a.** Click **Settings**. The **Public IP Address** window appears. **b.** Select an option. • **Use WAN interface**: When multiple WAN ports are available, you can select which WAN interface to use for monitoring IP changes. • **Assign static IP addresses**: myQNAPcloud binds the DDNS to the specified static IP address regardless of changes to the network environment. • **Automatically obtain IP address**: myQNAPcloud automatically detects the WAN IP. **c.** Click **Apply**.

Installing an SSL Certificate

Important
myQNAPcloud SSL web service and Let's Encrypt certificates can only be used with the myQNAPcloud domain.

1. Open myQNAPcloud.
2. Go to **SSL Certificate**.
3. Download and install a certificate.

Type	Description	User Action
myQNAPcloud SSL web service certificate	This certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users.	Hover the mouse pointer over **myQNAPcloud** and then click **Download and install**. **Important** To apply the SSL certificate, you must purchase the SSL Certificate License from QNAP Software Store and activate the license in License Center. This certificate should match the specified device region. For example, if your device region is set to `Global`, you must purchase a Global Domain license. For details, see Buying a License Using QNAP ID and License Activation.
Let's Encrypt certificate	Let's Encrypt is a free, automated, and open certificate authority that issues domain-validated security certificates. You can install Let's Encrypt certificates with the myQNAPcloud DDNS service. You can choose to automatically renew this certificate before it expires.	**a.** Hover the mouse pointer over **myQNAPcloud** and then click **Download and install**. The **Download & Install SSL Certificate** window appears. **b.** Specify a valid email address. This address is required for the Let's Encrypt account registration. **c.** Optional: Select **Automatically renew domain before expiration.** **d.** Click **Confirm**.

myQNAPcloud applies the certificate and displays the details.

Tip
To delete the certificate from the device, click **Remove**.

7. AMIZ Cloud

AMIZ Cloud is a cloud management platform that allows IT professionals to centrally deploy, operate, and monitor various devices, virtual machines, and containerized applications, providing flexible and reliable solutions for building and managing enterprise-level networks and IT infrastructure.

About AMIZ Cloud

AMIZ Cloud is designed for centrally managing various devices in the cloud. After creating an organization and specifying user roles, you can add devices to your organization by using an AMIZ Cloud join key or specifying hardware information. Owners and administrators in your organization can manage, operate, and configure connected devices and also deploy virtual machines or containers on these devices. You can create alert policies to receive notifications for specific events and view the comprehensive dashboard to monitor the status of your devices.

To access AMIZ Cloud, click  on the QNE task bar or go to https://amizcloud.qnap.com/ and sign in with your QNAP ID.

Important
You can only manage devices that are in Cloud Management Mode. For details, see Mode Selection.

Organization Setup

AMIZ Cloud and Organizations

Before you can start deploying devices, you must first set up an organization for your business in Organization Center. AMIZ Cloud automatically creates a default organization the first time you sign in to AMIZ Cloud using your QNAP ID. You can edit this organization or create more organizations for your business so that you can add devices to different organizations according to your needs. AMIZ Cloud supports managing and monitoring devices across multiple organizations.

Organization Privileges

Organization Center Account provides two user roles: organization owners and administrators. Owners can manage devices that belong to their own organizations. After creating an organization, you are the default owner of this organization. You can then invite users to your organization as administrators to help manage devices in this organization. You can also grant owner privileges to up to 200 administrators for each organization.

Creating an Organization

1. Go to https://organization.qnap.com/.
2. Sign in with your QNAP ID.
3. Click **Create Organization**.
4. Specify the following information.
   - **Organization name**
   - **Country**
   - **Size**: the number of members in your organization

- **Website**: the official website of your organization
- **Contact number**

5. Click **Next**.
6. Optional: Create a group.
   a. Click **Create Groups**.
      The **Create Groups** window appears.
   b. Specify a group name.
   c. Specify a description.
   d. Click **Create**.
7. Click **Next**.
8. Optional: Invite users to your organization as administrators.
   a. Click **Invite Administrators**.
      The **Invite Administrators** window appears.
   b. Specify the QNAP ID (email address or phone number) of a user.

Tip

You can click  to select a user from your contact list.

   c. Assign the user to a group.
   d. Click **Add**.

   Organization Center sends an invitation letter to the specified email address. After accepting the invitation, the user becomes an administrator of your organization.

9. Click **Done**.

The organization is created.

Managing an Organization

Organization owners can configure settings for their own organizations. Administrators can only view the information of organizations that they have joined.

1. Go to https://organization.qnap.com/.
2. Sign in with your QNAP ID.
3. Select an organization.
4. Perform one or more of the following tasks.

Task	User Action
Edit organization information	**a.** Click  . **b.** Select **Edit**. **c.** Specify the organization information. **d.** Click **Edit**.
Create a group for the organization	**a.** Click the **Group** section. **b.** Select the **Group** tab. **c.** Click **Create Groups**. The **Create Groups** window appears. **d.** Specify the group information. **e.** Select administrators. **f.** Click **Create**.
Create a site for the organization	**a.** Click the **Group** section. **b.** Click the **Site** section. **c.** Click **Create Site**. The **Create Site** window appears. **d.** Specify the site information. **e.** Click **Create**.
Invite users to the organization as administrator	**a.** Click the **Group** section. **b.** Select the **Account List** tab. **c.** Click **Invite Administrators**. The **Invite Administrators** window appears. **d.** Click **Invite Administrators**. **e.** Specify the QNAP ID and description of a user. **f.** Click **Add**. **g.** Add more users if needed. **h.** Click **Invite**.
Export the activity log	**a.** Click the **Group** section. **b.** Select the **Activity Log** tab. **c.** Click **Export Activity Log**. The **Export Activity Log** window appears. **d.** Specify a date range. **e.** Click **Apply**. **f.** Click **Download**.

Task	User Action
Edit administrator information	**a.** Click the **Administrators** section. **b.** Select the **Account List** tab. **c.** Select an administrator. **d.** Click  . The **Edit Administrator Information** window appears. **e.** Specify a description. **f.** Specify a status for the user. • **Active** • **Suspended**: A suspended administrator can no longer manage the devices of this organization. **g.** Grant or withdraw owner privileges. **h.** Click **Close**.
Remove a group, site, or administrator from the organization	**a.** Click the **Group** section. **b.** Select one of three tabs. • **Group** • **Site** • **Account List** **c.** Select one or more items from the list. **d.** Click **Delete**. A confirmation message appears. **e.** Click **Confirm**.

Deleting an Organization

You can delete an organization if you no longer need to access or manage the devices in this organization.

Warning
Once you delete your organization:

- All devices registered under this organization are removed.
- Your purchased licenses are permanently removed.
- All data associated with this organization is deleted and cannot be recovered.

1. Go to https://organization.qnap.com/.
2. Sign in with your QNAP ID.
3. Select an organization.

4. Click  .
5. Select **Remove**.
   The **Permanently Delete Organization** window appears.
6. Specify the organization name to confirm the request.
7. Select a reason for deleting this organization.
8. Leave a comment to add extra information.
9. Click **Verify through email**.
   Organization Center sends a confirmation email to the email address of the organization owner.
10. Open and review the email.

Important
You should fully understand the consequences of deleting this organization before proceeding to the next step.

11. Click **Delete Organization**.
    You are redirected to a confirmation page.
12. Read and agree to all terms.
13. Click **Confirm**.

Organization Center deletes the organization.

After deleting an organization, you can no longer manage the devices in this organization with AMIZ Cloud services. To centrally manage these devices in the cloud again, you must create another organization and add your devices to the organization.

Deployment

This section explains how to deploy containers, devices, and virtual machines on AMIZ Cloud.

Adding a Device Using Hardware Information

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Click **Add Devices**.
5. Click **Add**.
   The **Enter Hardware Information** window appears.
6. Configure the general settings.

Setting	User Action
Organization	Choose an organization for your device.
Hostname	Specify the hostname of your device.

Setting	User Action
myQNAPcloud device name	Specify a unique myQNAPcloud device name. **Note** If you do not specify a device name, an alphanumeric suffix is automatically added to the hostname to create a unique device name.
Description	Specify the device description.
Site	Select the preconfigured site from the drop-down menu. **Note** For details on creating a site in an organization, see Managing an Organization.

7. Configure the device initialization settings.

Setting	User Action
Username	Specify the device username.
Password	Specify the device password.
Confirm password	Verify the password.
Time zone	Select the device time zone from the following options. • **Select automatically** • **Select manually**
NTP server	Enter the network time protocol (NTP) server to synchronize the device clock with AMIZ Cloud organization time zone.

8. Enable **Automatically update the software components after configuring the basic settings**.
9. Click **Add Devices**.

AMIZ Cloud adds the hardware information of your device.

Adding a Device Using an AMIZ Cloud Join Key

You can also deploy your device by creating an AMIZ Cloud join key and sending the join key configuration to the device administrator. You can deploy the device once you initialize the device on the myQNAPcloud website.

Important
Ensure that the organization owner provides access control to your QNAP ID in myQNAPcloud in order to permit management of your devices on AMIZ Cloud.

1. Go to AMIZ Cloud.
2. Click **AMIZ Cloud Join Keys**.
3. Configure the join key settings.
   a. Click **Create AMIZ Cloud Join Keys**.
   The **Create AMIZ Cloud Join Keys** window appears.
   b. Click **Add**.

c. Configure the general settings.

Setting	User Action
Organization	Choose an organization for your device.
Hostname	Specify the hostname of your device.
myQNAPcloud device name	Specify a unique myQNAPcloud device name. **Note** If you do not specify a device name, an alphanumeric suffix is automatically added to the hostname to create a unique device name.
Description	Specify the device description.
Site	Select the preconfigured site from the drop-down menu. **Note** For details on creating a site in an organization, see Managing an Organization.

d. Specify the email recipient.

e. Select **Enable device initialization settings**.

f. Configure the device initialization settings.

Setting	User Action
Username	Specify the device username.
Password	Specify the device password.
Confirm password	Verify the password.
Time zone	Select the device time zone from the following options. • **Select automatically** • **Select manually**
NTP server	Enter the network time protocol (NTP) server to synchronize the device clock with AMIZ Cloud organization time zone.

g. Optional: Enable **Automatically update the software components after configuring the basic settings**.

h. Click **Create**.

myQNAPcloud sends an email to the device administrator with instructions on how to deploy the device.

4. Initialize the device on myQNAPcloud.

a. Open the myQNAPcloud email that contains the join key information.

b. Under QNAP Cloud Installation, click **Go to the page**.
The myQNAPcloud webpage containing the device information appears.

c. Click **Initialize**.
The **Smart Installation** window appears.

d. Follow the on-screen instructions of the wizard to complete the device initialization.

5. Initialize the device on AMIZ Cloud.

Note
Perform these steps only if you have created the AMIZ Cloud Join Key without configuring the device initialization settings.

   a. Go to AMIZ Cloud.

   b. Go to **Manage** > **AMIZ Cloud Join Keys** .

   c. Click  located next to the hostname of the unconfigured device.
   The **Device Initialization** window appears.

   d. Configure the device initialization settings.

Setting	User Action
Username	Specify the device username.
Password	Specify the device password.
Confirm password	Verify the password.
Time zone	Select the device time zone from the following options. • **Select automatically** • **Select manually**
NTP server	Enter the network time protocol (NTP) server to synchronize the device clock with AMIZ Cloud organization time zone.

   e. Click **OK**.

AMIZ Cloud deploys your device.

Deploying a Virtual Machine

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Click **Deploy Virtual Machines**.
   The **Deploy Virtual Machines** page appears.
5. Select an image from the QNAP Marketplace list.
6. Configure the image information.

   a. Under Select a Resource, click **Edit**.

   b. Configure the following.

Setting	User Action
VM name	Specify a name used to identify the VM

Setting	User Action
CPU allocation	Select one of the following for CPU allocation: • **Shared**: Shares the specified CPU resources with other applications. • **Dedicated**: Assign CPU resources specifically for this VM.
CPU	Specify the number of CPUs for the VM.
Memory	Specify the amount of memory required to run the VM.

c. Click **OK**.

7. Select the devices to deploy the VM on.

Tip
Beside Hostname, select the checkbox to select all devices.

8. Configure the VM settings.

Setting	User Action
Default settings	Enable the default VM settings preconfigured by the system.

Custom Settings	Enable to modify the VM settings based on your requirements. Configure the following:
	• **General**: Specify the VM description and enable **Start the VM automatically after creation**.
	• **Network**: Specify the number of network adapters required to deploy the VM.
	• **Others**
	  • **Restrict VM console access**: Restrict access to use the VM console for the standard VM user role. You can disable it by setting a VNC password.
	  • **Set VNC password**: Enable and specify the virtual network computing (VNC) password to encrypt the VM connection.

9. Click **Deploy Virtual Machines**.

AMIZ Cloud deploys the VM on the selected devices.

Cloning a Virtual Machine

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Click **Clone Virtual Machine**.
   The **Clone Virtual Machine** page appears.
5. Select a VM from the list of powered-off VMs.
6. Configure the VM resources.

Setting	User Action
VM name	Specify a name used to identify the VM
CPU allocation	Select one of the following for CPU allocation: • **Shared**: Shares the specified CPU resources with other applications. • **Dedicated**: Assign CPU resources specifically for the cloned VM.
CPU	Specify the number of CPUs for the VM.
Memory	Specify the amount of memory required to run the VM.

7. Configure the VM settings.

Setting	User Action
Default settings	Enable the default VM settings preconfigured by the system.

Custom Settings	Enable to modify the VM settings based on your requirements. Configure the following:
	• **General**: Specify the VM description and enable **Start the VM automatically after creation**.
	• **Others**
	  • **Restrict VM console access**: Restrict access to use the VM console for the standard VM user role. You can disable it by setting a VNC password.
	  • **Set VNC password**: Enable and specify the virtual network computing (VNC) password to encrypt the VM connection.

8. Click **Clone Virtual Machine**.

AMIZ Cloud clones the selected VM on the device.

Deploying a Container

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Click **Deploy Containers**.
   The **Deploy Containers** page appears.
5. Select an image or application from the QNAP Marketplace list.
6. Configure the image information.
   a. Under Specify Resources and Devices, click **Edit**.
   b. Configure the following.

Setting	User Action
CPU allocation	Select one of the following for CPU allocation: • **Shared**: Shares the specified CPU resources with other applications. • **Dedicated**: Assign CPU resources specifically for this container.
CPU	Specify the number of CPUs for the container.
Memory	Specify the amount of memory required to run the container.

c. Click **OK**.

7. Select the devices.

Tip
Beside Hostname, select the checkbox to select all devices.

8. Click **Deploy Containers**.

AMIZ Cloud deploys the container on the selected devices.

Duplicating a Container

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Click **Duplicate Container**.
   The **Duplicate Containers** page appears.
5. Select a container from the list.
6. Specify the container resources.

Setting	User Action
Container name	Specify the container name
CPU allocation	Select one of the following for CPU allocation: • **Shared**: Shares the specified CPU resources with other applications. • **Dedicated**: Assign CPU resources specifically for this container.
CPU	Specify the number of CPUs for the container.
Memory	Specify the amount of memory required to run the container.

7. Configure the container settings.

Setting	User Action
Default settings	Enable the default container settings.
Custom Settings	Enable to modify the container settings based on your requirements.

a. Configure the custom settings.

Setting	User Action
General	Configure the following: • Enable or disable **Pull the image from the registry before creating the container**. • **Memory reservation**: Reserve limited or unlimited memory for the container. • **Restart policy**: Specify the restart policy from the drop-down list.
Command	Configure the following: • **CMD**: You can specify the command to override the default instruction provided by the container image. • **Entrypoint**: Specify an entrypoint for running the container as an executable. • Enable **Allocate interactive and TTY processes for the container** to allow interactive processes (like a shell) run on the container. • Enable **Run the container in privileged mode** to allow the container access to all devices on the host machine. **Note** Privileged mode is disabled by default.
Networks	Configure the following: • **Hostname**: Specify the container network hostname. • **MAC address**: Specify the MAC address for the cloned container. **Tip** Click to generate a new MAC address. • **Exposed ports**: You can view the exposed network ports defined by the container image.
Environment	Click **Add Environment Variables** to define variables and values that can be used in the container commands and arguments.
Labels	Click **Add Label Key** to add metadata to the duplicated container.

Setting	User Action
Volumes	Click **Add Volume** to select from the following. • **New volume**: Specify a new volume and container for the duplicated container image. • **Container volume**: Select the volume from a preconfigured container. **Note** You can select the volume file system from the following. • **Read/Write** • **Read-only** • **Existing volume**: Select the volume from the existing list of volumes and define the path for the new container using the duplicated container image.

8. Click **Duplicate Container**.

AMIZ Cloud duplicates the container from the selected container image.

Management

This section explains how to manage deployed containers, devices, and virtual machines on AMIZ Cloud.

Managing Devices

1. Go to AMIZ Cloud.
2. Go to **Nodes** > **Devices** .
3. Select a device.
   The **Summary** page appears.
4. Click **Action**.
5. Manage the following device settings.

Setting	Description
Update Firmware	Checks and installs the latest firmware automatically. **Warning** Do not power off your device during the firmware update process. **Important** All ongoing tasks will be suspended during the auto update. However, to prevent loss of data, if there are any live iSCSI or Fibre connections to the device, or virtual machines running in Virtualization Station the device will not be able to automatically update the firmware.

Setting	Description
Update Software Components	Checks and installs the latest updates of all the software components installed on the device.
Restart	Restarts the device.
Shutdown	Shuts down the device.
Remove	Removes the device from the AMIZ Cloud portal. **Important** Removing the device will also unregister the device from myQNAPcloud.

Managing Virtual Machines

1. Go to AMIZ Cloud.
2. Go to **Nodes** > **Virtual Machines** .
3. Select a virtual machine.
   The **Summary** page appears.
4. Click **Action**.
5. Perform the following VM settings.

Setting	Description
Start	Starts a powered-off VM
Reset	Resets the VM
Shutdown	Performs an orderly shut down process on a running VM
Force Shutdown	Stops a running or unresponsive VM and forces it to shut down
Suspend	Writes the VM memory to the disk and puts the VM to sleep mode Suspending the VM saves its current state.
Resume	Resumes a VM from its suspended state
Take Snapshot	Creates a VM snapshot
Clone	Clones a powered-off VM
Remove	Removes the VM and its configuration from the device

Configuring VM Settings

1. Go to AMIZ Cloud.
2. Beside  , select an organization.
3. Go to **Nodes** > **Virtual Machines** .
4. Identify a virtual machine.
5. Click the VM name.
   The VM **Summary** page appears.
6. Go to **Information** > **General** .
7. Configure the following VM settings.

Important
Some settings are not accessible if the VM is running or suspended.

VM Settings	User Action
General	To configure the general VM settings, see Configuring General Settings. Configure the remaining settings. • **CPU Model**: The CPU model used by the virtual machine • **CPU Allocation**: Assign shared or dedicated CPU resources to the VM. • **Enable CPU Hot Add**: Allows you to add CPU resources to a running VM. For details, see here. • **Enable memory sharing**: Improves memory density on the host system by eliminating redundant copies of memory pages • **Enable dynamic memory allocation**:
Networks	To add a network device to the VM, see Adding a Network Device to a VM. To configure network settings, see Configuring Network Settings.
Storages	To add a storage device to the VM, see Adding a Storage Device to a VM.
CD/DVD	To configure CD/DVD settings, see Configuring CD/DVD Settings.
Console Operation	To configure the VM console operations, see Configuring Console Operation Settings.
Others	To configure VM auto start settings, see Configuring Other Settings.
Snapshots	To configure the VM snapshot settings, see Creating a VM Snapshot. To schedule a VM snapshot, see Enabling a VM Snapshot Schedule.
Logs	To monitor the VM logs, go to **[VM_Name]** > **Monitor** > **Logs** .

8. Click **Apply**.

AMIZ Cloud saves the VM settings.

Managing Containers

1. Go to AMIZ Cloud.
2. Go to **Nodes** > **Containers** .
3. Select a container.
   The **Summary** page appears.
4. Click **Action**.
5. Perform the following container settings.

Setting	Description
Start	Starts the created or stopped container
Restart	Restarts the running container
Stop	Stops the running container
Kill	Terminates the running container without saving any unsaved changes
Resume	Resumes a container from its paused state
Pause	Pauses the running container

Setting	Description
Duplicate	Duplicates the container
Remove	Removes the container and its configuration from the device

Configuring Container Settings

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Go to **Nodes** > **Containers** .
4. Identify a container.
5. Click the container name.
   The **Summary** page appears.
6. Go to **Information** > **General** .
7. Configure the following container settings.

Container Settings	User Action

General	Configure the general container settings.
	• **Container name**: Modify the container name.
	• **CPU**: The number of CPU cores used by the container.
	• **CPU allocation**: Assign shared or dedicated CPU resources to the container.
	• **Memory**: The maximum amount of memory available to the container.
	• **Memory reservation**: Reserve limited or unlimited memory for the container.
	• **Restart policy**: Select one of the following for the restart policy options:
	  • **None**: The container does not automatically restart.
	  • **On failure**: The container automatically restarts only if it exits due to an error.
	  • **Always**: The container automatically restarts even if it was previously stopped.
	  • **Unless stopped**: The container does not automatically restart if it was previously stopped.
	Note
	The restart policy determines whether or not a container also restarts when the server or application restarts.

Networks	View network-related settings of the container.
Volumes	Monitor the container volume information.
Logs	To monitor the container logs, go to **[Container_Name]** > **Monitor** > **Logs** .

8. Click **Apply**.

AMIZ Cloud saves the container settings.

Monitoring

After deploying devices, virtual machines, and containers, you can monitor their status on the AMIZ Cloud dashboard and create alert policies to receive notifications for specific system events. You can also view various logs, alerts, and task history to prevent or troubleshoot system issues for your organization.

Viewing the Dashboard

AMIZ Cloud dashboard displays key information on deployed devices, virtual machines, containers. The dashboard visualizes the numbers of recent alerts in a line chart, allowing you to effectively monitor the status of your IT infrastructure and quickly respond to potential issues.

You can choose to view devices in all your organizations or only those in a specific organization by clicking the drop-down list beside  . You can also specify a time range for the line chart of recent alerts.

Creating an Alert Policy

You can create alert policies in AMIZ Cloud to centrally monitor the CPU utilization, memory utilization, and network traffic on your devices. You can also send alert emails to specified recipients for system events. This allows IT administrators to respond promptly to potential system issues.

1. Go to AMIZ Cloud.
2. Next to  , select an organization.
3. Click **Actions**.
4. Select **Create Alert Policy**.

Tip
If this is the first time you create an alert policy, you can also click **Alert Policies** from the left navigation pane and then click **Create Alert Policy** on this screen.

The **Create Alert Policy** screen appears.

5. Specify a name and a description for this policy.
6. Specify alert criteria.
    a. Select a category.
    b. Specify an upper or lower threshold for the selected category.
    c. Select a duration.
    d. Select a severity level.
7. Select one or more devices.
8. Specify the email address of one or more alert recipients.
9. Click **Create Alert Policy**.

After creating an alert policy, you can view the policy from the alert list.

Note
You may not be able to view certain policy details on the alert list if you are not granted permissions to access that information.

To edit or remove an alert policy, click next to this policy, and select **Edit** or **Remove**.

Viewing Logs and Alerts

AMIZ Cloud displays various logs, alerts, and task history in a sliding window, allowing you to view important system events and operations in one place. By default, this window is minimized and hidden at the bottom of the main screen. To view the content in the window, you can click  to restore the window or click and hold  to drag the window to the desired height. To search for specific entries, click  and specify keywords.

8. HybridMount

HybridMount is a QNAP application that enables low-latency access to cloud storage through remote mounting of cloud services and remote devices. HybridMount also allows you to use caching for cloud services.

Installing HybridMount

Important
HybridMount is preinstalled on QNE. You can reinstall HybridMount to mount shared folders for File Station.

1. Log on to QNE as administrator.
2. Go to the **Application Store**, and then click .
   A search box appears.
3. Type `HybridMount`, and then press `ENTER`.
   The HybridMount application appears in the search results.
4. Click **Install**.
   QNE installs HybridMount.

Supported Cloud Services

HybridMount supports the following cloud services:

Cloud Services		
Alibaba Cloud Object Storage Service	Google Drive File Storage	Microsoft SharePoint
Amazon Simple Storage (Amazon S3)	hicloud S3	Oracle Cloud Infrastructure
Backblaze B2 Cloud Storage	HiDrive Cloud Storage	OVHcloud
Box Cloud Storage	HKT Cloud Storage	QCloud IT
Catalyst Cloud	Huawei Cloud Object Storage Service	Qiniu Cloud
Cynny Space: Cloud Object storage	IBM Cloud	Rackspace Cloud
DigitalOcean Object Storage	IONOS Cloud S3	S3 Compatible Storage
DirectCloud	luckycloud S3	OpenStack Swift
DreamObjects Cloud Storage	Microsoft Azure Storage	Wasabi Cloud Object Storage
Dropbox	Microsoft OneDrive for Business	WebDAV Cloud File Storage
Google Cloud Storage	Microsoft OneDrive's Personal Cloud Storage	Yandex.Disk

Remote Mounts

HybridMount provides two mounting modes to help you create a hybrid cloud environment on your device.

Mode	Description
File Cloud Gateway **Important** To mount more than two cloud services, you must purchase a license from the Software Store. To access the Software Store, go to **Licenses** > **Purchase License** .	File Cloud Gateway mode allows you to mount cloud services and access their data in File Station and through protocols such as SMB, NFS, WebDAV, and FTP. File Cloud Gateway mode also allows you to use caching for mounted cloud services by creating a cache space. **Note** HybridMount only allows the creation of cache spaces. For details, see Mounting a Cloud Service Using File Cloud Gateway.
Network Drive	Network Drive mode allows you to mount remote devices as network drives and access their data through various protocols. To see supported protocols, go to **Control Panel** > **Privilege** > **Shared Folders** . For details, see Mounting a Remote Device.

Mounting a Cloud Service Using File Cloud Gateway

File Cloud Gateway mode allows you to mount cloud services and use caching by creating a cache space.

Important
QNE can access files in cloud storage and download those files to the cache space on the device. You may incur additional data transfer costs.

1. Open **HybridMount**.
2. Click **Create Remote Mount**.
   A dialog box appears.
3. Click **Create File Cloud Gateway**.
   The **File Cloud Gateway Wizard** appears.

Tip
You can also access the wizard by navigating to the Overview screen and clicking **Create File Cloud Gateway** under **Cache Space**.

4. Select a cloud service.
5. Configure the selected cloud service.

Important
Depending on the selected cloud service provider, you may need to perform the following additional actions:

- Sign in, authenticate, or configure settings through a third-party interface.
- Select one or more folders as a destination folder.

6. Specify a connection name that contains 1 to 64 characters.
7. Select an upload policy.

Policy	Description
Check for conflicts and rename local files	Before uploading files, HybridMount checks if any of the files on the cloud have been modified by other users. If so, HybridMount renames the local versions of the modified files before uploading them so that important modifications are not overwritten in the cloud. **Important** • Selecting this option may affect update speed. • You may incur additional costs when checking files on the cloud.
Update files without checking	HybridMount overwrites existing files in the cloud without checking for modifications. QNAP recommends selecting this option if no other user access the cloud service account.

8. Optional: Configure the file list update schedule.
   You can set a schedule for automatically updating the list of cached files.

Note
This option is not available for some cloud services.

   a. Select **Enable scheduled updates for file lists**.

Note
If scheduled updates are disabled when the file list is created, HybridMount updates the list only once. You can manually update the file on the Mount Management screen.

   b. Select the frequency, days, and time period.

9. Click **Next**.

10. Create a cache space.

    a. Specify the capacity of the cache space.

    b. Click and drag the sliders to modify the proportion of allocated cache space.

       - **Maximum reserved cache**: Reserved cache is dedicated cache space for high-priority files, which are always kept in the local cache space.
       - **Maximum write cache**
       - **Minimum read cache**

11. Select an auto-download option.

    - **Pre-download all recently edited files**: This option automatically downloads all recently edited files.
    - **Download all new versions stored in the local cache**: This option automatically downloads modified versions of existing files in the local cache.
    - **Disable auto-download (Files will be downloaded only after they are accessed)**: This option does not automatically download any files.

12. Click **Create**.
    The summary screen appears.

> **Tip**
> This created mount automatically appears on the left panel of File Station. To hide a mount, go to **Control Panel** > **Privilege** > **Shared Folders** .

13. Click **Close**.

> **Tip**
> Click **Create More** to mount additional cloud services or remote devices.

14. Click **Close**.

Mounting a Remote Device

1. Open **HybridMount**.
2. Click **Create Remote Mount**.
   A dialog box appears.
3. Click **Create Network Drive Mount**.
   The **Network Drive Mount Wizard** window appears.
4. Perform one of the following actions.

Action	Steps
Manually specify the device	Specify the IP address, hostname, or webDAV URL of the device.
Select a device	**a.** Select a remote device from the table. **Tip** Click ↻ to refresh the device list. **b.** Specify the account name and password. **c.** Click **Connect**.

> **Tip**
> Click **Change Host** to specify a different remote device.

5. Select a protocol.

> **Note**
> If you select FTP or WebDAV, you cannot enable other file protocols in the Control Panel. For details, see Enabling File Protocols and File Station Access to Shared Folders.

Protocol	Description	User Actions
CIFS/SMB	Microsoft Networking (CIFS/SMB) supports online streaming and thumbnail display. It allows a single folder to be mounted through your local network or when the NAS connects with a VPN service.	**a.** Specify the following information. • Account name • Password • Destination folder • Connection name **b.** Optional: Select **Support multimedia playback and thumbnail display**. **Note** When selected, the system generates thumbnails and allocates storage space on the remote device.
FTP	FTP allows you to mount remote folders to your NAS for easier access to remote data. You can mount either the FTP root folder or a specific subfolder inside the FTP root folder.	**a.** Select a character encoding option. **b.** Specify the following information. • Port number • Account name • Password • Connection name **c.** Optional: Select **Secure connection (FTPS)**. **d.** Select one of the following options for the destination folder: • **All folders**: Mounts all folders in the remote device. • **Single folder**: Mounts one folder.
SFTP	SFTP provides secure file transfer capabilities via SSH.	Specify the following information. • Authentication method • Port number • Account name • Password or SSH private key • Destination folder • Connection name

Protocol	Description	User Actions
WebDAV	Accessing files through WebDAV is similar to downloading files from a webpage as they both use the same tunnel. It allows a single folder to be mounted through a local network or over the internet. WebDAV uses the HTTP protocol and the same HTTP port.	**a.** Specify the following information. • Account name • Password • Connection name **b.** Select an upload policy: • **Check for conflicts and rename local files** • **Update files without checking** **c.** Optional: Select **Enable scheduled updates for file lists** and specify an update schedule. **d.** Click **Next**. **e.** Create a cache space. For details, Mounting a Cloud Service Using File Cloud Gateway.
NFS	Network File System (NFS) allows you to access files on a remote device as if they were local files.	**a.** Select one of the following options for the destination folder: • **All folders**: Mounts all folders in the remote device. • **Single folder**: Mounts one folder. **b.** Specify the connection name.

Tip
You can also configure protocol settings in **Control Panel** > **Privilege** > **Shared Folders** .

6. Click **Create**.
   The summary screen appears.
7. Click **Close**.

Note
Click **Create More** to mount additional remote devices.

The mounted device appears on the **Remote Devices** screen in HybridMount and in File Station as a network drive.

Tip
To hide a mount, go to **Control Panel** > **Privilege** > **Shared Folders** .

Mount Management

The **Mount Management** screen displays all mounted cloud services and remote devices and provides access to configuration options.

The following table lists types of connection statuses.

Status	Description
Disabled	The connection is disabled.
Failed	HybridMount failed to connect to the remote device or cloud service.
Invalid	A connection configuration error occurred. The cloud service or remote device must be remounted.
Mounted	The cloud service or remote device is mounted and ready for use.
Mounting	HybridMount has created the connection and is currently mounting the cloud service or remote device.

The following table lists types of cache statuses and only applies to cloud mounts.

Status	Description
	The list of cached files is up-to-date.
	HybridMount is updating the list of cached files.
	An error occurred while updating the list of cached files.  **Tip** For details about the error, click  .

Managing a Cloud Service Mount

Managing a File Cloud Gateway Mount

1. Open HybridMount.
2. Click **Mount Management**.
3. Locate a File Cloud Gateway mount to manage.
4. Perform one of the following actions.

 **Important**
You can still view and delete connections for disabled cloud mounts.

Action	Steps
Reauthenticate the cloud service account	**a.** Click  . **b.** Follow the on-screen instructions to complete the reauthentication.  **Note** This action is only available when the connection status is "Invalid" and HybridMount cannot connect to the cloud service due to an authentication error.

Action	Steps
View cache space information	Under **Cache Space**, click ⚙. The **Cache Space** window appears. You can view the following information: • Real-time status of the cache space: location, total capacity, allocated read, write, and reserved cache, and free space. • Used storage space for the past seven days.
Configure advanced cache settings	**a.** Under **Cache Space**, click ⚙. The **Cache Space** window appears. **b.** Click **Advanced Cache Settings**. **c.** Click and drag the sliders to modify the proportion of cache space allocated to **Maximum reserved cache**, **Maximum write cache**, and **Minimum read cache**. **d.** Configure the **Auto-download setting**. **e.** Click **Apply**.
View connection information	**a.** Click **More**. **b.** Select **Information**. The connection information appears.
Update the list of cached files for the connection	**a.** Click **More**. **b.** Select **Update Now**. **Note** This option is only available for object cloud storage connections.
Edit connection settings	**a.** Click **More**. **b.** Select **Edit**. The **Edit Mount** window appears. **c.** Modify the settings. **d.** Click **Apply**.
View file upload information	**a.** Click **More**. **b.** Select **Uploads**. The **Uploads** window appears. From this window, you can view the upload status of each file and the list of upload errors.
Perform a speed test	**a.** Click **More**. **b.** Select **Speed Test**. The **Speed Test** window appears. **c.** Click **Speed Test**. The system performs a speed test and displays the results. **d.** Click **Close**.

Action	Steps
Modify cache priority settings	**a.** Click **More**. **b.** Select **Cache Priority**. The **Cache Priority** window appears. **c.** Click a cached folder. **d.** Select a priority level. • **Always keep in reserved cache**: Files are always kept in the local cache. • **Normal**: Least-accessed files are removed first. • **Low priority**: Low-priority files are removed first. **Note** Lowering the priority of infrequently used folders allows more efficient use of the cache volume. **e.** Click **Apply**.
Configure upload and download speed limits	To reduce system load, you can configure upload and download speed limits when the device is in heavy use. **a.** Click **More**. **b.** Select **Rate Limit**. **c.** Under **Upload Speed**, select one of the following: • **Unlimited**: Do not limit the upload speed. • **Maximum**: Limit the upload speed to between 1 and 1024 Kbps or Mbps. **d.** Under **Download Speed**, select one of the following: • **Unlimited**: Do not limit the download speed. • **Maximum**: Limit the download speed to between 1 and 1024 Kbps or Mbps. **e.** Configure the schedule for enforcing speed limits. • **Always-on**: Enforce the speed limits at all times. • **Specified time**: Enforce the speed limits according to the specified start time, end time, and days of the week.
Delete the connection	**a.** Click **More**. **b.** Select **Delete**. A confirmation message appears. **c.** Click **Yes**.

Managing a Network Drive Mount

1. Open HybridMount.
2. Click **Mount Management**.
3. Locate a Network Drive mount to manage.
4. Perform one of the following actions.

Important
You can still view and delete connections for disabled cloud mounts.

Action	Steps
View connection information	**a.** Click **More**. **b.** Select **Information**. The connection information appears.
Edit connection settings	**a.** Click **More**. **b.** Select **Edit**. The **Edit Mount** window appears. **c.** Modify the settings. **d.** Click **Apply**.
Perform a speed test	**a.** Click **More**. **b.** Select **Speed Test**. The **Speed Test** window appears. **c.** Click **Speed Test**. The system performs a speed test and displays the results. **d.** Click **Close**.
Delete the connection	**a.** Click **More**. **b.** Select **Delete**. A confirmation message appears. **c.** Click **Yes**.

Managing a Remote Device Mount

1. Open HybridMount.
2. Click **Mount Management**.
3. Click **Remote Devices**.
4. Locate the mount you want to manage.
5. Perform one of the following actions.

Action	Steps
View connection information	**a.** Click **More**. **b.** Select **Information**. The connection information appears.
Edit connection settings **Note** You cannot perform this action if you disable the mount.	**a.** Click **More**. **b.** Select **Edit**. The **Edit Mount** window appears. **c.** Modify the settings. **d.** Click **Apply**.
Delete the connection	**a.** Click **More**. **b.** Select **Delete**. A confirmation message appears. **c.** Click **Yes**.

Remounting a Connection

Remounting a past connection allows you to easily use similar protocols or minimal changes to a connection you want to mount again.

Note
You can only remount deleted mounts.

1. Open HybridMount.
2. Click **Logs**.
   A menu list appears.
3. Select **Mount Logs**.
4. Locate the connection you want to remount.
5. Click .

Note
If you remount a cloud service, you may need to log on, authenticate, or configure settings through a third-party interface.

6. Optional: Configure the settings.
7. Click **Apply**.
   A confirmation message appears.
8. Click **OK**.

Adjusting Total Concurrent Upload and Download Files

When multiple cloud mounts are available, you can optimize file transfers by configuring specific settings.

1. Open HybridMount.
2. Click **Transfer Resource Management**.

3. Perform one of the following actions.

Action	Steps
Edit concurrent transfer files **Note** This option ensures that a guaranteed number of concurrent files are allocated to a mount.	**a.** Locate a cloud mount you want to modify. **b.** Click . The **Edit Concurrent Transfer Files** screen appears. **c.** Modify the settings. **d.** Click **Apply**.
Set specific conditions for high-priority transfers **Note** This option ensures that a specific file size or file type is prioritized in file transfers.	**a.** Locate a cloud mount you want to modify. **b.** Click . The **Priority Transfer Settings** window opens. **Note** To configure priority transfer settings for downloads, click **Download**. **c.** Click **Add Condition**. **d.** Select one of the following options. • **File size** • **File type** **e.** Configure the settings. **f.** Click **Save**.
Set concurrent upload or download files provided to HybridMount.	**a.** Click **Settings**. The **Concurrent Transfer File Settings** window opens. **b.** Specify the maximum number of concurrent upload or download files. **c.** Click **Apply**.

Logs

HybridMount maintains and displays three types of logs: mount logs, speed test logs, and event logs.

Log Type	Description
Mount logs	These logs contain the summary of all successfully mounted remote devices and cloud services.
Speed test logs	These logs contain the summary of all speed tests performed for each mounted connection.
Event logs	These logs contain the summary of all cache-related events.

Managing Mount Logs

On the **Mount Logs** screen, you can view the latest 200 mount logs.

You can also remount devices or cloud services on this screen. For details, see Remounting a Connection.

1. Open HybridMount.
2. Go to **Logs** > **Mount Logs** .
3. Select an action to perform.

Action	Steps
Delete a mount log	**a.** Identify a log to delete. **b.** Under **Action**, click .
Delete multiple mount logs	**a.** Select logs to delete. **b.** Click **Delete**.

Managing Speed Test Logs

On the **Speed Test Logs** screen, you can view the 50 latest speed test logs per connection.

1. Open HybridMount.
2. Go to **Logs** > **Speed Test Logs** .
3. Optional: Filter the list by connection.
   a. Click **All connections**.
   b. Select a connection.
   The screen displays speed test logs for the selected connection only.
4. Select an action to perform.

Action	Steps
Delete a speed test log	**a.** Identify a log to delete. **b.** Under **Action**, click .
Delete multiple speed test logs	**a.** Select logs to delete. **b.** Click **Delete**.

Managing Event Logs

On the **Event logs** screen, you can view event logs by severity level, search event logs using keywords, and copy and delete event logs.

You can also configure notification settings. For details, see the Notification Center section of the QNE User Guide.

1. Open HybridMount.
2. Go to **Logs** > **Event Logs** .
3. Select an action to perform.

Action	Steps
Copy an event log	**a.** Right-click a log. **b.** Select **Copy**.
Delete an event log	**a.** Right-click a log. **b.** Select **Delete this record**.
Filter by severity level	**a.** Next to **Severity Level**, click **All severity levels**. **b.** Select a severity level.
Search by keyword	Enter keywords in the **Content search** box.

9. File Station

File Station is a file management application that allows you to access files across NAS devices and cloud services. This application requires HybridMount to mount a share folder or a cloud drive to File Station. Any changes you make are reflected in your cloud drive or across all of your devices that have this share folder. For more information on HybridMount, see HybridMount.

Getting Started

1. Install HybridMount.

Note
HybridMount is a preinstalled application on QNE.

For details, see Installing HybridMount.

2. Create a remote mount.

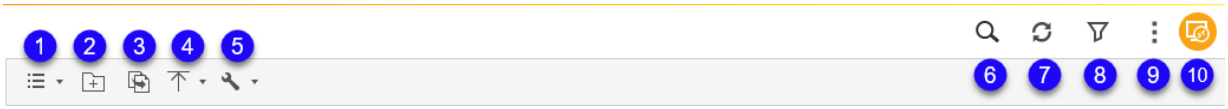
Note
To create a remote mount directly in File Station, click **Remote Mount** on the toolbar. For details on how to create a remote mount, see Remote Mounts.

Installing File Station

1. Log on to QNE.
2. Go to the **Application Store**, and then click .
   A search box appears.
3. Type `File Station`, and then press **ENTER**.
   The File Station application appears in the search results.
4. Click **Install**.
   QNE installs File Station.

Parts of File Station

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

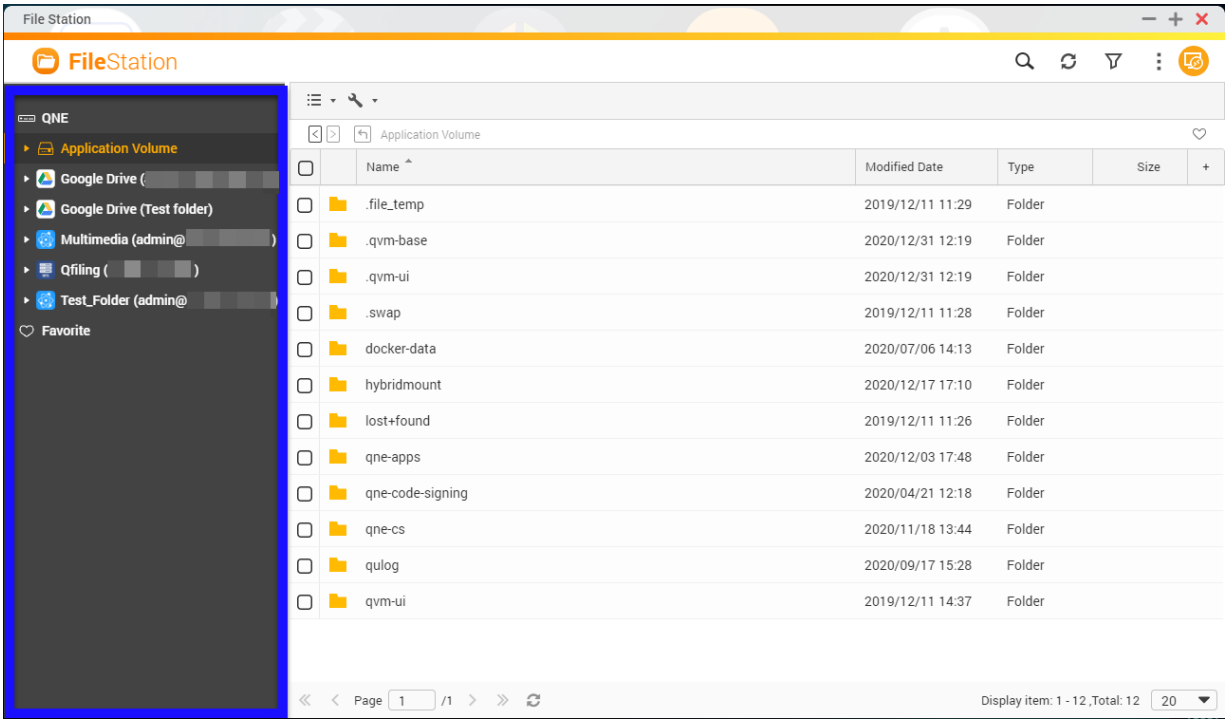


Toolbar Tasks

Label	Item	Description
1	Browsing Mode	Select a browsing mode.
2	Create folder	Create a folder inside a network drive mount. **Note** This button is not available for cloud mounts.

Label	Item	Description
3	Copy	Copy the selected files and folders. **Note** This button only appears when a file or folder is selected.
4	Upload	Upload files or folders to the selected shared folder. **Note** This button is not available for cloud mounts.
5	More Actions	Perform different tasks. **Note** Some task options only appear when you select certain types of files.
6	Search	Search files and folders by their name or type. **Tip** You can select **Advanced Search** to specify more criteria.
7	Refresh	Refresh the current page.
8	Smart Filter	Filter files and folders based on the specified criteria.
9	More Settings	Configure the File Station settings
10	Remote Mount	Manage files across local, external, remote, and cloud storage resources on a single interface. To use this feature, install HybridMount from the Application Store. For more information on HybridMount, go to HybridMount.

The left panel displays all of your mounts. You can show or hide mounts from the Control Panel. For details, see Enabling File Protocols and File Station Access to Shared Folders.



Depending on the mount and the location of shared folders, you can perform various tasks from the left panel.

To perform an action on the left panel, right-click a mount.

Tip
Hover your mouse over a mount to see the name and its protocol.

Left Panel Tasks

Task	Description
Create folder	Creates a new folder in the mount.
Copy	Copies the mount.
Open	Opens the mount.
Download	Downloads the mount to your computer.
Rename	Renames the shared folder.
Copy to / Move to	Copies or moves a shared folder to a different location.
Cut	Moves the shared folder to a different location. **Note** After selecting a different location for the shared folder, this option removes the shared folder from the old mount.
Delete	Deletes the shared folder.

Task	Description
Add to Favorites	Adds a mount for the shared folder in the **Favorite** section. **Tip** To remove a folder from this section, right-click on the folder and click **Remove from Favorites**.
Compress	Compresses the shared folder.
Properties	Views the mount or folder properties.

Supported File Formats

The supported file formats are categorized in alphabetical order.

Category	File Extension
Image	• BMP • GIF • JPE • JPG • PNG • TGA
Music	MP3
Video	MP4

File and Folder Transfer

This section describes tasks related to transferring your files and folders to the NAS or to a different device.

Uploading Files and Folders

You can either add files or folders one at a time or add several at once. However, you can only upload files or folders to a subfolder mounted on a cloud service.

1. Open File Station.
2. Open the destination folder.
3. Drag and drop files and folders from your computer to the destination folder.

Tip

You can upload files or folders separately. Click and select **File** or **Folder**. Select the files or folders you want to upload and then click **Open** or **Upload**.

The **Background Task** window opens.

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

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

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

5. Click **OK**.
   File Station uploads the selected items.

Downloading Files and Folders

You can download files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Click **Download**.
Using the left panel **Note** This option downloads all items in a mount.	**a.** Right-click a mount. **b.** Click **Download**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Click **Download**.

File Station downloads the items to your computer.

File and Folder Access

This section describes tasks related to accessing your files and folders.

Creating a Folder

You can only create a folder in mounts created by file protocols or in a folder on a mounted cloud service. You cannot create a folder in a shared folder that's mounted separately by a cloud service.

1. Open File Station.
2. Locate the destination mount.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click . The **Create Folder** window opens. **b.** Specify the folder name. **c.** Click **OK**.
Using the left panel	**a.** Right-click the mount. **b.** Select **Create Folder**. The **Create Folder** window opens. **c.** Click **OK**.

File Station creates a new folder.

Deleting Files and Folders

Important
Deleted files are removed permanently.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Note
If the shared folder you want to delete is part of a cloud mount, you can right-click the folder from the left panel and select **Delete**. If the shared folder is mounted separately, you cannot delete the folder from the left panel.

Method	Steps
Using the toolbar	**a.** Click . **b.** Select **Delete**. A confirmation message appears. **c.** Click **OK**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Delete**. A confirmation message appears. **c.** Click **OK**.

File Station deletes the selected items permanently.

Opening a File

1. Open File Station.
2. Locate and select a file.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Click **Open**.
Using the left panel	Right-click and then select **Open**.
Opening the file directly	Double-click the file.

File Station opens the selected file.

Opening a Text File Using Text Editor

This task requires that you install Text Editor from the Application Store. You can only open one text file at a time.

1. Open File Station.
2. Locate and double-click the text file.

Tip
You can also right-click the file and click **Open with Text Editor**.

File Station opens the selected text file using Text Editor.

Opening Multimedia Files Using Media Viewer

Media Viewer is an application that allows you to play videos, listen to music, and view photos in File Station. Without Media Viewer, multimedia files open in a new browser on your computer.

To open multimedia files using Media Viewer, you must complete the following steps.

- Install Media Viewer from the Application Store.
- Ensure that File Station supports the multimedia file format. For details, see Supported File Formats.
- Ensure that multimedia files are located within a CIFS/SMB mounted shared folder.

Note
Opening multimedia files that are located in other mounts opens the file in a new browser.

- Select **Support multimedia playback and thumbnail display** in the mount settings and in General Settings in File Station. To select the option in General Settings, see Modifying General Settings.

1. Open File Station.
2. Locate and select a multimedia file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Play**.

Method	Steps
Using the context menu	**a.** Right-click the file. **b.** Select **Play**.
Opening the file directly	Double-click the file.

File Station opens the file using Media Viewer.

Tip
To download music or video files to your computer, click and then click **Download**.

Viewing the File or Folder Properties

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click . **b.** Select **Properties**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Properties**. **Tip** If the folder you want to view appears on the left panel, you can right-click the folder from the left panel and select **Properties**.

Depending on your selected items, the **Properties** window opens and displays the following information.

Field	Description
Selected items	Displays how many items are selected.
Type	Displays the folder or file type.
Size	Displays the file or folder size. **Tip** If you selected multiple items, click to display the total size and file count.
File Path	Displays the file or folder location.
Modified Date	Displays the date the file or folder was last modified.

4. Click .

File and Folder Organization

This section describes tasks related to organizing your files, folders, and mounts.

Sorting Files and Folders

Sort files and folders to make them easier to see and find.

1. Open File Station.
2. Click .
3. Select one the following.
   - List
   - Large icons
   - Medium icons
   - Small icons

   File Station displays files and folders according to the selected option.
4. Click a column title.

> **Note**
> This option is only available in the list view.

File Station sorts files in an ascending or descending order based on the selected column.

Copying Files and Folders

You can copy files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Copy to / Move to** and then select **Copy to**. The **Folder Selector** window opens. **c.** Select the destination folder. **d.** Select a mode. **e.** Optional: Select **Merge selected file transfer tasks**. **f.** Click **Apply**.
	a. Click  . **b.** Go to the destination folder. **c.** Click  .
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Copy**. **c.** Go to the destination folder. **d.** Right-click inside the folder and then select **Paste**. **Note** You can aslo right-click a folder from the left panel and select **Paste**.
Using drag and drop	**a.** Select the file. **b.** Drag and drop to the destination folder. Step result: A context menu appears. **c.** Select one of the following actions. • **Copy and skip duplicate files** • **Copy and overwrite duplicate files** • **Copy and rename duplicate files**
Using keyboard shortcuts	**a.** Press **CTRL + C** or **Command-C**. **b.** Go to the destination folder. **c.** Press **CTRL + V** or **Command-V**.

Method	Steps
Using the left panel **Note** This option applies to subfolders.	**a.** Right-click a subfolder. **b.** Hover your mouse over **Copy to/ Move to**, and then select **Copy to**. The **Folder Selector** window opens. **c.** Select a destination folder. **d.** Optional: Select a mode. **e.** Optional: Select **Merge selected file transfer tasks**.
Using the left panel **Note** This action applies to mounts.	**a.** Right-click a mount. **b.** Select **Copy:/MOUNTNAME**. **c.** Go to the destination folder. **d.** Click .

File Station creates a copy of the selected items.

Moving Files and Folders

You can only move subfolders underneath a mount. You can move files or folders either individually or in batches.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click . **b.** Select **Copy to / Move to** and then select **Move to**. The **Folder Selector** window opens. **c.** Select the destination folder. **d.** Specify a mode. **e.** Optional: Select **Merge selected file transfer tasks**. **f.** Click **Apply**.

Method	Steps
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Right-click the file and then select **Copy to/Move to** and **Move to**. The **Folder Selector** window opens. **c.** Select the destination folder. **d.** Select a mode. **e.** Optional: Select **Merge selected transfer tasks**. **f.** Click **Apply**.
	a. Right-click a selected file or folder and then select **Cut**. **b.** Select the destination folder. **c.** Right-click inside the folder and then select **Paste**.
Using the left panel	**a.** Right-click a subfolder. **b.** Hover your mouse over **Copy to/ Move to**, and then select **Move to**. The **Folder Selector** window opens. **c.** Select a destination folder. **d.** Optional: Select a mode. **e.** Optional: Select **Merge selected file transfer tasks**. **f.** Click **Apply**.

File Station moves the selected items to the specified folder.

Renaming Files or Folders

You can only rename one file or folder at a time.

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

Note
If the shared folder you want to rename is part of a cloud mount, you can right-click the folder from the left panel and select **Rename**. If the shared folder is mounted separately, you cannot rename the folder from the left panel.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Rename**.
Using the context menu	**a.** Right-click the file or folder. **b.** Select **Rename**.

The **Rename** window opens.

4. Specify a file or folder name.
5. Click **OK**.
   File Station renames the file or folder.

Compressing Files and Folders

Compressing files and folders are not applicable to shared folders mounted by a cloud service. If you want to compress items in a specific shared folder on a cloud service, you must mount your entire cloud drive and access that specific folder through the mounted drive.

Note
If the shared folder you want to compress is part of a cloud mount, you can right-click the folder from the left panel and select **Compress**. If the shared folder is mounted separately, you cannot compress the folder from the left panel.

1. Open File Station.
2. Locate and select one or more files and folders.
3. Perform one of the following methods.

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

The **Compress** window opens.

4. Configure the file compression settings.

Option	Task
Archive name	Specify a name for the compressed file.
Compression level	Select the type of compression method. • **Normal** - Standard compression • **Maximum compression** - Prioritizes compression quality • **Fast compression** - Prioritizes compression speed
Archive format	Select the format of file compression. • **zip** • **7z**

Option	Task
Update mode	Specify how the files should be updated. • **Add and replace files** • **Update and add files** • **Update existing files** • **Synchronize files**

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

Extracting Compressed Files and Folders

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

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

4. Select one of the following file extraction options.

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

   A confirmation message appears.

5. Select whether to overwrite the existing file.
   File Station extracts the compressed files to the specified folder.

Encrypting Files

1. Open File Station.
2. Locate and select one or more files.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Encrypt**. The **Encrypt** window opens. **c.** Specify a password. **d.** Verify the password. **e.** Select a mode. **f.** Select whether to encrypt and replace the original file. **g.** Click **OK**.
Using the context menu	**a.** Locate a file in the list and then right-click. **b.** Select **Encrypt**. The **Encrypt** window opens. **c.** Specify a password. **d.** Verify the password. **e.** Select a mode. **f.** Select whether to encrypt and replace the original file. **g.** Click **OK**.

Decrypting Files

This task decrypts files directly in File Station. You can also use the QENC Decrypter to decrypt files. To download the QENC Decrypter, visit https://www.qnap.com/en/utilities/enterprise.

1. Open File Station.
2. Locate and select an encrypted file.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Decryption**. The **Decryption** window opens. **c.** Specify the password. **d.** Select a mode. **e.** Click **OK**.

Method	Steps
Using the context menu	**a.** Right-click the encrypted file. **b.** Select **Decryption**. **c.** Specify the password. **d.** Select a mode. **e.** Click **OK**.

Adding a Mount to the Favorite Section

To find a mount faster, you can add a folder to the favorites section. You can only add a mount the **Favorite** section. You cannot add folders within a mount to this section.

1. Open File Station.
2. Locate and select the mount you want to add.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Add to Favorites**. **Note** You can also click ♡ near the right corner of the toolbar.
Using the left panel	**a.** Right-click the mount. **b.** Select **Add to Favorites**.

The mount appears as a folder under **Favorite**.

Removing a Mount from the Favorite Section

1. Open File Station.
2. Under **Favorite**, locate and select the mount you want to remove.
3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **Note** You can also click ♥ near the right corner of the toolbar. **b.** Select **Remove from Favorites**.

Method	Steps
Using the left panel	**a.** Right-click the mount. **b.** Select **Remove from Favorites**.

The mount is removed from the **Favorite** section.

File Station Navigation

This section describes tasks related to finding your files and folders on File Station.

Searching for Files and Folders

You can only search for files and folders in a specific mount. To search in a different mount, see Using Advanced Search to Search for Files and Folders.

1. Open File Station.
2. Near the top-right corner, click .
   A search box appears.
3. Specify a file or folder name.
4. Optional: Select a file or folder type.
   a. Click .
      A menu list appears.
   b. Select one of the following options.
      - **Any**
      - **Music**
      - **Video**
      - **Photo**
      - **Advanced Search**
        For more information on **Advanced Search**, see Using Advanced Search to Search for Files and Folders.
5. Press ENTER.

Using Advanced Search to Search for Files and Folders

Advanced Search allows you to search for files and folders in a different mount.

1. Open File Station.
2. Near the top-right corner, click .
   A search box appears.
3. Click .
   A menu list appears.
4. Select **Advanced Search**.

The **Advanced Search** screen appears.

5. Specify at least one of the following fields.

Field	Description
Name	Searches by file or folder name.
Size	Searches a file or folder greater than or less than a specified size.
Modified Date	Searches before, on, or after a specific date or a date within a range.
Location	Searches for files and folders in a specific mount.
Type	Searches by a file type.

6. Optional: Select **Filter based on the rules specified above**.

Note
This option autmatically turns on the **Smart File Filter**. When the **Smart File Filter** is enabled, it applies the specified criteria to all of your mounts. For details on the **Smart File Filter**, see Using the Smart File Filter to Search for Files and Folders.

7. Click **Search**.

Using the Smart File Filter to Search for Files and Folders

The **Smart File Filter** allows you to apply a set of search criteria to all of your mounts. When you click a mount, the feature automatically filters your files and folders by the search criteria.

1. Open File Station.
2. Near the top-right corner, click .
   The **Smart File Filter** screen appears.
3. Specify at least one of the following fields.

Field	Description
Name	Searches by file or folder name.
Size	Searches a file or folder greater than or less than a specified size.
Modified Date	Searches before, on, or after a specific date or a date within a range.
Type	Searches by a file type.

4. Click **Search**.
   File Station turns on the **Smart File Filter** and filters by the specified criteria.

Other Tasks

This section describes miscellaneous tasks that you can perform on File Station.

Adding a File to a Reserved Cache

This task only applies to mounts that use a cache space. Adding a file to a reserved cache treats the file as high priority and ensures that they are cached in advance. For details, see Managing a Cloud Service Mount.

1. Open File Station.
2. Locate and select one or more files and folders.

3. Perform one of the following methods.

Method	Steps
Using the toolbar	**a.** Click  . **b.** Select **Always Keep in Reserved Cache**.
Using the context menu	**a.** Locate a file or folder in the list and then right-click. **b.** Select **Always Keep in Reserved Cache**.

File Station adds the selected items to the reserved cache.

Tip
For details on the different types of cache statuses, click next to **Cache Status**.

Removing Background Tasks

You can remove background tasks that aren't necessary or stop them from running.

1. Open File Station.
2. Click  .
3. Select **Background Task**.

Tip
The **Task** tab displays all tasks. The **Upload** tab only displays upload tasks. To see your upload tasks, click **Upload**.

4. Locate a task you want to remove.
5. Click .
File Station removes the task.

Tip
To remove all tasks, click **Delete All**. To remove all completed tasks from the **Upload** tab, click **Remove All Complete Tasks**.

Modifying General Settings

1. Open File Station.
2. At the top left-corner, click **More Settings** ( ).
3. Click **Settings**.
The **Options** window opens.
4. Optional: Select at least one of the following options.

Option	Description
Show hidden files	Shows files or folders that are usually created to hold information. These are usually temporary folders or files.

Option	Description
Support multimedia playback and show thumbnails for photos	Allows media files to be played using Media Viewer. **Note** You must select this setting to open image files or play multimedia files using Media Viewer.

5. Click **Apply**.

Modifying File Transfer Settings

This task allows you to specify how File Station manages files and folders with the same names.

1. Open File Station.
2. At the top left-corner, click **More Settings** (⋮).
3. Click **Settings**.
   The **Options** window opens.
4. Click **File Transfer**.
5. Under **When uploading files** and **When copying or moving files**, select one of the following options.
   - **Always ask me**
   - **Rename duplicate files**
   - **Skip duplicate files**
   - **Overwrite duplicate files**
6. Optional: Select **Always merge all file transfer processes into one task.**

Tip
Selecting this option combines copying or moving multiple items into one task in the **Background Task**. If you do not select this option, each item appears as a single task in the **Background Task**.

7. Click **Apply**.

10. Virtualization Station

Virtualization Station centralizes the creation, configuration, and control of virtual machines on your QNAP device. A virtual machine (VM) allows you to run different virtualized software applications, such as operating systems or software routers, in a secure environment on your device.

VM and VA Creation

Virtualization Station allows you to create VMs, import VM files, and deploy virtual appliances (VAs) from the VM Marketplace.

Creating a VM

1. Open Virtualization Station.
2. Go to **Overview**.
3. Click **Create VM**.
   The **Create VM** window opens.
4. Configure the VM settings.

Setting	Description
VM Name	The name used to identify the VM Requirements: • Length: 1–32 characters • Not allowed: Name cannot start with a Space ( ). • The following special characters are not allowed: ` * = + [ ] \ | ; : ' " , < > / ? %
Description	The description for the VM
OS Type	The type of operating system used by the VM
OS Version	The operating system version used by the VM
Boot Firmware	The type of firmware used during the boot sequence

Setting	Description

CPU	The CPU resource available to the VM
	• Click **Specify CPU Resources**.
	The Specify CPU Resources window appears.
	• Select a method.
	  • **Shared**: The threads can be shared with other services.
	  • **Dedicated**: The current service occupies the threads until you modify the settings.
	• Select a processor.
	Note
	This setting is available only if your device supports more than one processor.
	• Select the number of cores and threads.
	• Click **Apply**.

Memory	The maximum amount of memory available to the VM
Enable Memory Sharing	Improves memory density on the host system by eliminating redundant copies of memory pages
Installer Disc (.iso)	The ISO image used to create the VM **Tip** A disk image must be added to the **Images** section before it is available here.
Virtual Disk Size	The maximum amount of storage available to the VM on the virtual disk
Start the VM automatically after creation	Virtualization Station automatically starts the VM after you create it.
Advanced Settings	
Network	The network interface used by the VM **Tip** To add a new network interface, click .
Restrict VM console access	Blocks all access to the VM console **Note** This option is only available when a VNC password is set.
Set VNC Password	Sets a VNC password VNC passwords are used to access the desktop for VMs. Requirements: • Length: 1 - 8 characters • Valid characters: A–Z, a–z, 0–9 • Valid special characters: Hyphen (-), Underscore (_), Period (.)

5. Click **OK**.

Virtualization Station creates the VM.

Importing a VM

1. Open Virtualization Station.
2. Go to **Overview**.
3. Click **Import VM**.
   The **Import VM** window opens.
4. Click  .
   A file explorer window opens.
5. Select the VM file.

Important
Virtualization Station only imports the following file types:

- .ova
- .ovf
- .vmx
- .qvm

6. Click **Open**.
   The file explorer window closes.
7. Click **Next**.
8. Configure the VM settings.

Setting	Description
VM Name	The name used to identify the VM Requirements: • Length: 1–32 characters • Not allowed: Name cannot start with a Space ( ). • The following special characters are not allowed: ` * = + [ ] \ | ; : ' " , < > / ? %
Description	The description for the VM

Setting	Description

CPU	The CPU resource available to the VM
	• Click **Specify CPU Resources**.
	The Specify CPU Resources window appears.
	• Select a method.
	  • **Shared**: The threads can be shared with other services.
	  • **Dedicated**: The current service occupies the threads until you modify the settings.
	• Select a processor.
	Note
	This setting is available only if your device supports more than one processor.
	• Select the number of cores and threads.
	• Click **Apply**.
	Important
	You cannot configure shared and dedicated CPU resources for devices supporting less than four cores and eight threads.

Memory	The maximum amount of memory available to the VM

9. Optional: Configure the advanced settings.
   a. Click **Advanced Settings**.
   b. Modify any of the following settings.

Setting	Description
CPU	The CPU model used by the virtual machine **Tip** This setting is typically used when exporting the VM to another device.
Network	The MAC address and NIC model used by the VM **Tip** Click  to generate a MAC address.
Hard Disk	The path to the image file, cache mode, and drive controller type used by the VM storage

10. Click **Import**.

Virtualization Station imports the VM.

Deploying a Virtual Appliance from the VM Marketplace

The VM Marketplace provides access to several ready-to-use applications packaged as virtual appliances. From here you can download and deploy an existing a virtual appliance to your device.

1. Open Virtualization Station.
2. Go to **VM Marketplace**.
3. Identify a VM.
4. Click **Deploy**.
5. Configure the VM settings.

Setting	Description
VM Name	The name used to identify the VM
Description	The description for the VM

CPU	The CPU resource available to the VM
	• Click **Specify CPU Resources**.
	The Specify CPU Resources window appears.
	• Select a method.
	  • **Shared**: The threads can be shared with other services.
	  • **Dedicated**: The current service occupies the threads until you modify the settings.
	• Select a processor.
	Note
	This setting is available only if your device supports more than one processor.
	• Select the number of cores and threads.
	• Click **Apply**.
	Important
	You cannot configure shared and dedicated CPU resources for devices supporting less than four cores and eight threads.

Memory	The maximum amount of memory available to the VM
Enable Memory Sharing	Improves memory density on the host system by eliminating redundant copies of memory pages
Start the VM automatically after creation	Virtualization Station automatically starts the VM after you create it.
Network	The network interface used by the VM **Tip** To add a new network interface, click .

Setting	Description
Restrict VM console access	Blocks all access to the VM console **Note** This option is only available when a VNC password is set.
Set VNC Password	Sets a VNC password VNC passwords are used to access the desktop for VMs. Requirements: • Length: 1 - 8 characters • Valid characters: A–Z, a–z, 0–9 • Valid special characters: Hyphen (-), Underscore (_), Period (.)

6. Click **OK**.

Virtualization Station deploys the VA.

VM Management

Virtualization Station lists any VMs operating on the device. After selecting a VM, you can view detailed information, configure settings, access snapshots, and review logs for each VM.

VM Actions

Virtualization Station lets you perform a number of different actions related to the management and configuration of your VM.

Performing General VM Actions

The following tasks are commonly used when managing VMs with Virtualization Station.

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
   The VM Information screen appears.
4. Perform any of the following tasks:

Task	User Action
Access the VM console	Click .
Clone the VM	**a.** Click . The **Clone VM** window opens. **b.** Optional: Configure the VM settings. **c.** Click **OK**.

<table>
<tr><th>Task</th><th>User Action</th></tr>
<tr><td>Delete the VM</td><td>a. Click  .
The Delete Virtual Machine window opens.
b. Click OK.</td></tr>
<tr><td>Reset the VM</td><td>a. Click  > Reset .
A dialog box opens.
b. Click OK.
 
Note
This task only works on VMs that are currently running.</td></tr>
<tr><td>Start the VM</td><td>Click  .
 
Note
This task only works on VMs that are not currently running.</td></tr>
<tr><td>Stop the VM</td><td>a. Click  .
b. Select a shutdown option.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Shutdown</td><td>Sends an ACPI shutdown signal to the VM</td></tr><tr><td>Force Shutdown</td><td>Immediately shuts down the VM</td></tr></table>A dialog box opens.
c. Click OK.</td></tr>
<tr><td>Suspend the VM</td><td>Click  .</td></tr>
<tr><td>Resume the VM</td><td>Click  .</td></tr>
</table>

Virtualization Station performs the specified action.

Adding Hardware Devices to a VM

Adding hardware devices to a VM lets you expand its capabilities.

Adding a CD/DVD ROM to a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a powered off VM.
   The VM Information screen appears.
4. Go to **Settings**.

5. Click **Add Device**.
   The **Add Device** window opens.
6. Select the **CD / DVD ROM** device type.
7. Configure device settings.

Setting	Description
Image Path	The path to the ISO image file **a.** Click  . The **Connect CD-ROM** window opens. **b.** Select an ISO image file. **c.** Click **OK**.
Interface	The connection type for the storage device

8. Click **OK**.

Virtualization Station adds the device.

Adding a Network Device to a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.

Note

- You cannot add a network device to a suspended VM.
- You can only add VirtIO network devices to a running VM.

The VM Information screen appears.

4. Go to **Settings**.
5. Click **Add Device**.
   The **Add Device** window opens.
6. Select the **Network** device type.
7. Configure device settings.

Setting	Description
Model	The model of the network adapter
Physical Function	The specific PCIe network expansion card being added. **Important** This setting is only available when **Model** is set to **SR-IOV passthrough**.

Setting	Description
Enable Multiqueue	Multiqueue improves the networking performance by distributing network traffic within the NIC. **Important** This setting is only available when **Model** is set to **VirtIO**.
MAC Address	The MAC address for the network adapter **Tip** Click  to generate a MAC address.

8. Click **OK**.

Virtualization Station adds the device.

Adding a Storage Device to a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.

Note

- You cannot add a network device to a suspended VM.
- You can only add VirtIO network devices to a running VM.

The VM Information screen appears.

4. Go to **Settings**.
5. Click **Add Device**.
   The **Add Device** window opens.
6. Select the **Hard Disk** device type.
7. Configure device settings.

Setting	Description
Interface	The connection type for the storage device
Cache Mode	The cache mode of the storage device
Size	The maximum amount of storage available to the VM on the first virtual disk

8. Click **OK**.

Virtualization Station adds the device.

Connecting a USB Device to a VM

1. Open Virtualization Station.

2. Go to **VM List**.
3. Select a VM.
   The VM Information screen appears.
4. Click  .
   The **Connect USB Device** window opens.
5. Select a connected USB device.
6. Click **OK**.

Virtualization Station connects the USB device to the VM.

Connecting an Intel QAT Accelerator to a VM

Intel QuickAssist Technology (QAT) devices allows the creation of several virtual functions (VFs) to accelerate cryptographic functions and workload compressions by offloading the data to the connected hardware that can support optimization. QAT devices supports this acceleration by using Single Root I/O Virtualization (SR-IOV).

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a powered off VM.
   The VM Information screen appears.
4. Next to Intel QAT, click  .
   The **Connect to Intel® QAT Accelerator** window appears.
5. Specify the number of VF connections.

Note
One physical function (PF) corresponds to 16 VFs.

6. Click **OK**.

Virtualization Station saves the settings.

Connecting an ISO file to a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
   The VM Information screen appears.
4. Click  .
   A menu opens.
5. Click **(Empty)**.
   The **Connect CD-ROM** window opens.
6. Select an uploaded ISO file.

7. Click **OK**.

Virtualization Station connects the ISO file.

Ejecting an ISO image from a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
   The VM Information screen appears.
4. Click  .
   A menu opens.
5. Select the connected ISO file.
   The **Eject CD Image** window opens.
6. Click **OK**.

Virtualization Station ejects the ISO file.

Exporting a VM

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
   The VM Information screen appears.
4. Click  .
   The **Export VM** window opens.
5. Configure file settings.

Setting	Description
Export File Name	The name used for the export file
Format	The format of the export file

6. Optional: Configure additional settings.

Setting	Description
Include iso images	Includes an ISO image with the export file
Compress images	Compresses the export file  **Note** This setting is only available if you select the .qvm format.

Setting	Description
Stream-optimized format	Compresses the export file to a single growable format for streaming. **Note** This setting is only available if you select the .ovf format.

7. Click **Start**.
   Virtualization Station prepares the exported VM.
8. Go to the **Logs** tab.
9. Identify the successful export log.
10. Click .

Tip

Alternatively, you can go to **Notifications** > **Events** , and then click to download the exported VM.

Virtualization Station downloads the exported VM.

VM Settings

You can configure a variety of settings for each VM. These settings can control the resources available to the VM or how the VM interacts with the host device.

Important
Some settings are not accessible if the VM is running or suspended.

Configuring General Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **General** .
5. Optional: Configure the settings.

Setting	Description
VM Name	The name used to identify the VM Requirements: • Length: 1–32 characters • Not allowed: Name cannot start with a Space ( ). • The following special characters are not allowed: ` * = + [ ] \ | ; : ' " , < > / ? %

Setting	Description
CPU Model	The CPU model used by the virtual machine **Tip** This setting is typically used when exporting the VM to another device.
Hide KVM Hypervisor Signature	Hides the KVM hypervisor signature from the guest OS

Cores	The CPU resource available to the VM
	
	• Click **Specify CPU Resources**.
	The Specify CPU Resources window appears.
	• Select a method.
	  • **Shared**: The threads can be shared with other services.
	  • **Dedicated**: The current service occupies the threads until you modify the settings.
	• Select a processor.
	
	Note
	This setting is available only if your device supports more than one processor.
	
	• Select the number of cores and threads.
	• Click **Apply**.
	
	Important
	You cannot configure shared and dedicated CPU resources for devices supporting less than four cores and eight threads.

Memory	The maximum amount of memory available to the VM
Enable Memory Sharing	Improves memory density on the host system by eliminating redundant copies of memory pages
Enable dynamic memory allocation	Analyzes and allocates the appropriate amount of memory to a VM based the current system and VM needs

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Boot Settings

The boot order defines the devices and order in which the VM searches for boot files. These boot files can control how the VM operates.

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Boot Options** .

5. Optional: Configure the settings.

Setting	Description
Boot Firmware	The type of firmware used during the boot sequence **Note** The installed guest operating system may become unbootable after changing the boot firmware.
Boot Devices	The boot order of the VM.

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Network Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Network** .
5. Optional: Configure the settings.

Setting	Description
MAC Address	The MAC address for the network adapter **Tip** Click  to generate a MAC address.
Model	The model of the network adapter
Enable Multiqueue	Multiqueue improves the networking performance by distributing network traffic within the NIC. **Important** This setting is only available when **Model** is set to **VirtIO**.

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Storage Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Storage** .
5. Optional: Configure the settings.

Setting	Description
Size	The maximum amount of storage available to the VM on the first virtual disk
Cache Mode	The cache mode of the storage device
Interface	The connection type for the storage device

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring CD/DVD Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **CD/DVD** .
5. Optional: Configure the settings.

Setting	Description
Image Path	The path to a connected ISO image file **Tip** You can also eject the iso file from here.
Interface	The type of interface for the connected image file

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Video Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Video** .
5. Optional: Configure the type of video driver for the VM.
6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Audio Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.

4. Go to **Settings** > **Audio** .
5. Optional: Click **Enable audio** to add an emulated Intel High Definition Audio device to the VM.

Important
For some older operating systems, such as Windows XP, you must separately install drivers for the device.

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Console Operation Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Console Operation** .
5. Under **Language**, select the layout of the VM keyboard interface.
6. Configure the remote console.

Setting	Description
VM Console Port	Sets the port used to access the VM Console • **Auto port**: Virtualization Station automatically assigns an available port number to the VM console. • **Custom port**: Assign a custom port number between 5900 and 5930.
Restrict VM console access	Restricts login access to the VM console.
Set VNC Password	Sets a VNC password VNC passwords are used to access the desktop for VMs. Requirements: • Length: 1 - 8 characters • Valid characters: A–Z, a–z, 0–9 • Valid special characters: Hyphen (-), Underscore (_), Period (.)
Enable SPICE	Enables SPICE on the VM SPICE is a remote connection tool that supports audio transmissions.

7. Click **Apply**.

Virtualization Station saves the settings.

Configuring USB Settings

1. Open Virtualization Station.
2. Go to **VM List**.

3. Select a VM.
4. Go to **Settings** > **USB** .
5. Optional: Select the USB version.

Important

- USB 3.0 is only available on VMs running Windows 8 or later.
- If drivers are not installed for connected USB devices, the device may not function correctly.

6. Click **Apply**.

Virtualization Station saves the settings.

Configuring Other Settings

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Settings** > **Other** .
5. Optional: Configure the settings.

Setting	Description
Auto Start Policy	Automatically restarts the VM after the host restarts **Tip** • If you select **None**, you have to manually start the VM in case the device restarts. • Specify the startup delay between 0 and 600 seconds if you select **Retain previous status** or **Always**. • Online VMs are suspended before the host shuts down or reboots. VMs that use SATA controllers are shut down using an ACPI signal.
Enable Virtio-serial	Enables communication between the host and virtual machine After enabling this setting, the QNAP Guest Agent can collect virtual machine IP addresses and synchronize VM clocks. **Tip** Insert the Guest Tool CD image to install the QNAP Guest Agent.

6. Click **Apply**.

Virtualization Station saves the settings.

VM Snapshot Management

Snapshots allow your QNAP device to record the state of the VM at any time. If an unexpected situation arises on your system, you can revert back to a previous state that the snapshot has recorded. You can create and manage separate snapshots for each VM.

Creating a VM Snapshot

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Click **Take Snapshot**.
   The **Take Snapshot** window opens.
6. Configure the snapshot settings.

Setting	Description
Name	The name used to identify the snapshot Requirements: • Length: 1–32 characters • Not allowed: Name cannot start with a Space ( ). • The following special characters are not allowed: ` * = + [ ] \ | ; : ' " , < > / ? %
Description	The description for the snapshot
Reserve this snapshot	Retains the snapshot **Note** Virtualization Station deletes the oldest non-reserved snapshot after the system reaches the maximum number of snapshots (32).

7. Click **OK**.

Virtualization Station creates the snapshot.

Reverting to a VM Snapshot

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Identify a snapshot file.
6. Click  .

The **Revert** window opens.

7. Optional: Select **Synchronize the time of the host**

Important
Time synchronization will not take effect if the snapshot was taken before you enabled Virtio-serial and installed the QNAP Guest Agent on the VM.

8. Click **OK**.

Important
Reverting a virtual machine to a snapshot removes all USB connections.

Virtualization Station reverts the virtual machine.

Reserving a VM Snapshot

Tip
Reserving a snapshot prevents it from being deleted when the maximum number of snapshots is reached.

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Locate an unreserved snapshot file.
6. Click .

Virtualization Station reserves the snapshot.

Unreserving a VM Snapshot

Tip
Reserving a snapshot prevents it from being deleted when the maximum number of snapshots is reached.

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Locate a reserved snapshot file.
6. Click .

Virtualization Station unreserves the snapshot.

Deleting a VM Snapshot

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Select a snapshot file.

Important
You can only select non-reserved snapshots.

6. Click **Delete**.
   The **Delete Snapshot** window opens.
7. Click **OK**.

Virtualization Station deletes the snapshot file.

Enabling a VM Snapshot Schedule

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Click **Schedule**.
   The **Schedule** window opens.
6. Select **Enable Schedule**.
7. Configure the snapshot settings.

Note
Virtualization Station deletes the oldest non-reserved snapshot after the system reaches the maximum number of snapshots (32).

Setting	Description
Name	The name used to identify the snapshot Requirements: • Length: 1–32 characters • Not allowed: Name cannot start with a Space ( ). • The following special characters are not allowed: ` * = + [ ] \ | ; : ' " , < > / ? %
Description	The description for the snapshot
Repeat	Controls how often snapshots are created
Time	Controls what time to create snapshots

8. Click **OK**.

Virtualization Station enables the snapshot schedule.

Disabling a VM Snapshot Schedule

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Snapshots**.
5. Click **Schedule**.
   The **Schedule** window opens.
6. Deselect **Enable Schedule**.
7. Click **OK**.

Virtualization Station disables the snapshot schedule.

VM Log Management

Important events, errors, or warnings are recorded for each VM. These logs can be used to diagnose issues or monitor VM operations.

1. Open Virtualization Station.
2. Go to **VM List**.
3. Select a VM.
4. Go to **Logs**.
5. Perform and of the following tasks:

Task	User Action
Save VM log files	Click **Save**.
Delete VM log files	**a.** Click **Clear All**. The **Clear All Logs** window opens. **b.** Click **OK**.

Virtualization Station performs the specified task.

Image File Management

Within Virtualization Station, you can upload image files to your QNAP device. Image files are integral to the creation of virtual machines and can control how a VM operates.

1. Open Virtualization Station.
2. Go to **Images**.
3. Perform any of the following tasks:

Task	User Action
Upload an image file	**a.** Click **Upload Image**. The **Upload Image** window opens. **b.** Specify a description. Requirements: • Length: 1–32 characters **c.** Upload an image file. **Tip** Virtualization Station only accepts ISO image files. **1.** Click . A file explorer window opens. **2.** Locate an image file. **3.** Click **Open**. The file explorer window closes. **4.** **d.** Select a duplicate file rule. **e.** Click **OK**.
Edit an image file	**a.** Select an image file. **b.** Click **Edit**. The **Edit** window opens. **c.** Optional: Modify the description. **d.** Click **OK**.
Delete an image file	**a.** Select an image file. **b.** Click **Delete**. The **Delete Image** window opens. **c.** Click **OK**.

Virtualization Station performs the specified task.

Application Preferences

You can configure memory and language settings within Virtualization Station that are applied to all VMs running on your QNAP device.

Configuring Memory Preferences

1. Open Virtualization Station.
2. Go to **Preferences** > **Memory** .
3. Configure system memory provisioning.

Option	Description
Memory Reservation	Reserves a specified amount of memory dedicated to operating your QNAP device Using this option ensures that your device has enough memory to run smoothly and that VMs do not use excessive memory. **Important** By default, this setting is set to **None**. This allocates all memory to running virtual machines, but might result in insufficient memory for your QNAP device.
Memory Overcommitment	Allows you to allocate more virtual memory to VMs than is present on the physical device **Important** To ensure services run correctly, QNAP recommends using an overcommitment ratio of less than 50%.

4. Optional: Enable the **Memory Optimizer**.

Note
The memory optimizer controls memory usage for both the physical system and any VMs. This feature allows Virtualization Station to achieve higher memory density on the system by utilizing additional CPU consumption to merge identical memory and dynamic guest memory allocation.

   a. Click **Enable memory optimizer**.

5. Click **Apply**.

Virtualization Station saves the memory settings.

Configuring Language Preferences

1. Open Virtualization Station.
2. Go to **Preferences** > **Language** .
3. Select a language option.

Virtualization Station applies the selected language option.

Log Management

Important events, errors, or warnings are recorded for both Virtualization Station and any installed virtual machines. You can filter logs by type or search for specific log files. These logs can be used to diagnose issues or monitor VM operations.

1. Open Virtualization Station.
2. Go to **Log**.
3. Perform any of the following tasks:

Task	User Action
Search log files	**a.** Locate the **Search** field. **b.** Enter search terms.
Save log files	**a.** Click **Save**.  **Tip** You can filter the log files by searching before you save.
Delete log files	**a.** Click **Clear All**. The **Clear All Logs** window opens. **b.** Click **OK**.

Virtualization Station performs the specified task.

11. Ubuntu Linux Station

About Ubuntu Linux Station

Ubuntu Linux Station is an Ubuntu Linux operating system installation tool for your QNAP device. Integrated with Linux containers, it helps you to easily download and install lightweight fully-virtualized Linux OS images.

The application also allows you to configure the system settings of the installed OS and provides access to the built-in Virtual Network Computing (VNC) remote desktop feature.

Installation and Configuration

Installing an Ubuntu Operating System

Ubuntu Linux Station allows you to download an OS image from the Linux Containers website and install it on your QNAP device.

You can install one of the following operating systems:

- Ubuntu 18.04 (Bionic Beaver)
- Ubuntu 20.04 (Focal Fossa)

1. Open Ubuntu Linux Station.
2. On the side menu, select the operating system version.
3. Click **Install**.
   Ubuntu Linux Station installs and enables the operating system.

Configuring an Ubuntu Operating System

You can configure a variety of settings after installing the Ubuntu OS. These settings allow you to manage the resources available to the installed OS.

Configuring CPU and Memory Resources

1. Open Ubuntu Linux Station.
2. Configure the CPU resources.
   a. Under Resources, click  .
   The **CPU Resource Allocation** window appears.
   b. Configure the CPU allocation method.

Setting	Description
Shared	Shares the specified CPU resources with other applications.
Dedicated	Assign CPU resources specifically for this VM.

   c. Select a processor.

Note
This setting is available only if your device supports more than one processor.

d. Select the number of cores and threads.

e. Click **Apply**.

Important
You cannot configure shared and dedicated CPU resources for devices supporting less than four cores and eight threads.

3. Specify the amount of memory required to run the OS.
4. Click **Apply**.

Ubuntu Linux Station saves the CPU and memory resources.

Accessing the Ubuntu Remote Desktop

1. Open Ubuntu Linux Station.
2. Select the display resolution.
3. Select **Enable remote desktop**.
4. Select a method to view the remote desktop.
   - Click the connection URL
   - Beside the title, click .

   The Ubuntu remote desktop login page appears.
5. Select a user account.
6. Enter the password.
7. Press Enter on the keyboard.
8. On the side menu, perform the following actions.

Setting	User Action
	Restart the Ubuntu operating system.
	Click to view the desktop in high resolution.
	Click to view the desktop in medium resolution.
	Click to view the desktop in low resolution.
	Enter the remote desktop fullscreen mode.
	Exit the remote desktop fullscreen mode.

9. Follow the wizard to configure the Ubuntu account settings and install applications.

Note
Account settings vary depending on the Ubuntu OS you have installed.

Configuring Network Adapter Settings

1. Open Ubuntu Linux Station.
2. Select a pre-configured virtual switch for network 1.
3. Optional: Configure a second network adapter.
   a. Click **Enable network connection**.
   b. Select a pre-configured virtual switch.

Tip
To configure a new virtual switch, click **Configure virtual switches**.

4. Click **Apply**.

Ubuntu Linux Station saves network settings.

Synchronizing User Credentials

You can synchronize the login credentials of the Ubuntu Linux operating system with the user credentials of the current administrator account.

1. Open Ubuntu Linux Station.
2. Under Overview, click  .
   The **Synchronize credentials** window appears.
3. Click **OK**.

Ubuntu Linux Station synchronizes the user credentials.

Performing Actions on an Ubuntu OS

1. Open Ubuntu Linux Station.
2. Perform an action on the OS.

Task	Description	Action
Enable the OS	Use to enable the Ubuntu OS.	On the **Overview** screen, click  .
Disable the OS	Use to disable the Ubuntu OS.	On the **Overview** screen, click  .
Restart the OS	Use to restart the OS. Use this feature if the OS becomes unresponsive.	On the main screen, click **Restart**.
Reinstall the OS	Use to reinstall the OS. Use this feature if the OS is corrupt or if a feature is missing.	On the main screen, click **Reinstall**.

Task	Description	Action
Uninstall the OS	Use to uninstall the OS.	On the main screen, click **Uninstall**.

12. Container Station

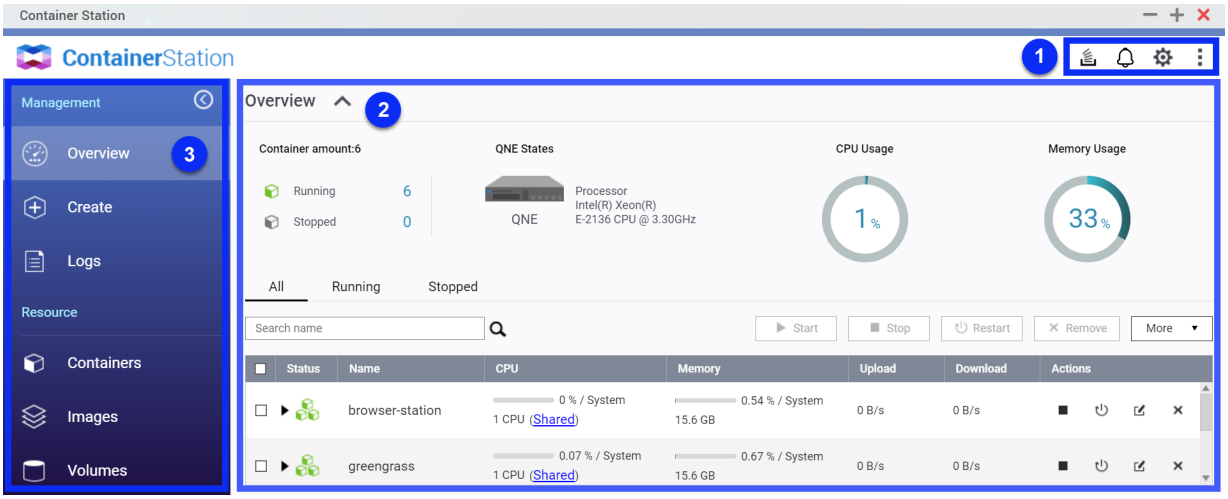
Overview

About Container Station

Container Station lets you install and centrally manage Docker containers on your QNAP device. Containers are a lightweight way to simulate a variety of operating systems and application services. Integrated with the Docker Hub Registry, Container Station helps you easily download ready-to-use images and increase the functionality of your QNAP device.

Parts of the User Interface

The Container Station user interface has three main areas.



Label	Area	Description

1	Toolbar	The toolbar displays the following buttons:
		• **Background Tasks**: Click to view the list of background tasks.
		• **Event Notifications**: Click to view the list of notifications.
		• **Settings**: Click to configure the notification rules.
		For details on adding event notification rules, see the Notification Center Help on QNE.
		• **More**: Click and then select one of the following:
		  • **Help**: Opens the Container Station Help panel.
		  • **About**: Displays the Container Station version.

2	Menu	The menu has two sections: Management and Resource. You can click or to collapse or expand the menu.
3	Main panel	The main panel displays the selected screen.

Container Creation

There are several ways to create containers in Container Station.

Creating a Container from a Recommended Application

The **Recommended** tab displays a list of QNAP apps and other recommended applications.

1. On the menu, click **Create**.
   The **Create** screen displays.
2. Go to the **Recommended** tab.
3. Select an application from the list and then click **Install**.
   An installation wizard displays.
4. Specify the allocated resources and then click **Create**.
   Container Station creates the container and installs the application.

Creating a Container from a Docker Hub Image

Container Station has a built-in Docker Hub where you can find Docker containers.

1. On the menu, click **Create**.
   The **Create** screen displays.
2. Go to the **Docker Hub** tab.
3. Type a keyword and then press **Enter** or click  .
   The list of available images appear.
4. Select an image from the list and then click **Install**.
   The **Select Image Version** window opens.
5. Select an image version and then click **Next**.
   The **Create Container** wizard opens.
6. Configure the container settings.
   Container Station provides default settings, which you can either retain or modify.
   For details on the available settings, see Editing the Container Settings.
7. Optional: Modify the advanced settings.
   This option is available for more advanced users.
   For details, see Modifying the Advanced Settings.

Important
You cannot modify the advanced settings after the container has been created.

8. Click **Next**.
   The **Summary** screen displays.
9. Review the container settings and then click **Create**.
   Container Station creates the container.

Creating a Container from an Existing Image

You can create a container from images that you have already pulled from Docker Hub or you can pull new ones, as needed.

1. On the menu, click **Images**.
   The **Images** screen displays.
2. Optional: Pull an image from Docker Hub.
   a. Click **Pull**.
      The **Pull image from registry** window opens.
   b. Type an image name.
      Image names must start and end with a letter or number, and can contain between 1 and 128 characters of the following types:
      - Letters: a–z
      - Numbers: 0–9
      - Special characters:
        - Hyphen (-)
        - Underscore (_)
        - Period (.)
        - Forward slash (/)
        - Colon (:)

Note
Using consecutive special characters in the image name is not allowed.

   c. Specify the image version.
      Image versions must start with a letter, number, or underscore (_), and can contain between 1 and 128 characters of the following types:
      - Letters: A–Z, a–z
      - Numbers: 0–9
      - Special characters:
        - Hyphen (-)
        - Underscore (_)
        - Period (.)
   d. Optional: Enable **Set to default**.
   e. Click **Pull**.
3. Locate an image from the list and then click + in the **Actions** column.
   The **Create Container** wizard opens.
4. Configure the container settings.

Container Station provides default settings, which you can either retain or modify.

5. Optional: Modify the advanced settings.
   This option is available for more experienced users.
   For details, see Modifying the Advanced Settings.

Important
You cannot modify the advanced settings after the container has been created.

6. Click **Next**.
   The **Summary** screen displays.

7. Review the container settings and then click **Create**.
   Container Station creates the container.

Creating an Application

Applications are multi-container resources created using Docker Compose. This is commonly used when a container may have dependencies and require other containers to function. To run applications, you can use a YAML file to describe components and configuration files.

1. On the menu, click **Create**.
   The **Create** screen displays.

2. Click **Create Application**.
   The **Create Application** window opens.

3. Configure the application settings.

   a. Specify the application name.

   b. Enter the Docker Compose YAML.
      For details, see https://docs.docker.com/compose/.

Tip
You can select and view `YAML` samples from the **Sample** drop-down list.

4. Optional: Click **Validate YAML** to verify if the code is correct.
   Container Station validates the YAML and highlights any formatting errors.

5. Click **Create**.
   Container Station creates the Docker Compose application.

Modifying the Advanced Settings

The advanced settings provide more granular options for intermediate users of Container Station.

Important
You cannot modify the advanced settings after the container has been created.

1. On the **Create Container** wizard, click Advanced Settings >> ▾ .
   The **Advanced Settings** section expands.

2. Optional: Modify any of the following settings.

Tab	Possible User Actions
Command	**a.** Specify the command line program and entrypoint. **Note** Use shell or exec syntax. **b.** Enable **Allocate interactive and tty processes for the container**. **c.** Enable **Run containers in privileged mode**.
Network	**a.** Specify the container hostname. **b.** Specify the container MAC address. **c.** Click **Add port forwarding rules** to open QNE Network Manager and add the port forwarding rules.. **d.** Enable **Use static IP**.
Environment	Click **Add** to specify environment variables.
Labels	Click **Add** to specify labels.
Volume	Click **Add volume** and then select one of the following: • **New volume** • **Volume from container** • **Existing volume**

Resource Management

Container Station allows you to manage containers, images, and volumes without leaving the application.

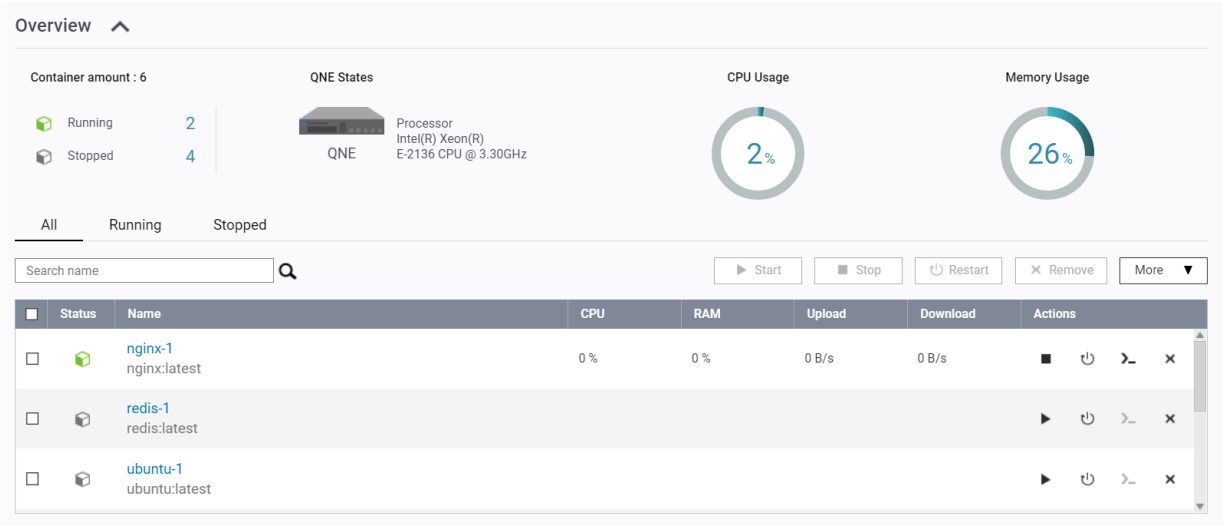
In some cases, you can also launch the QNE Network Manager from Container Station to modify advanced network settings that affect your containers. These settings enable you to more easily configure your infrastructure and manage the different resources that you need to run your containers.

Managing Containers

Container Station enables you to edit some container information, reallocate resources, modify the network settings, and perform actions on your containers after you create them.

Viewing the Container Station Dashboard

The Container Station **Overview** screen shows a dashboard with the QNE states, CPU usage, and memory usage. The screen also displays a searchable list of the containers that were created on Container Station.

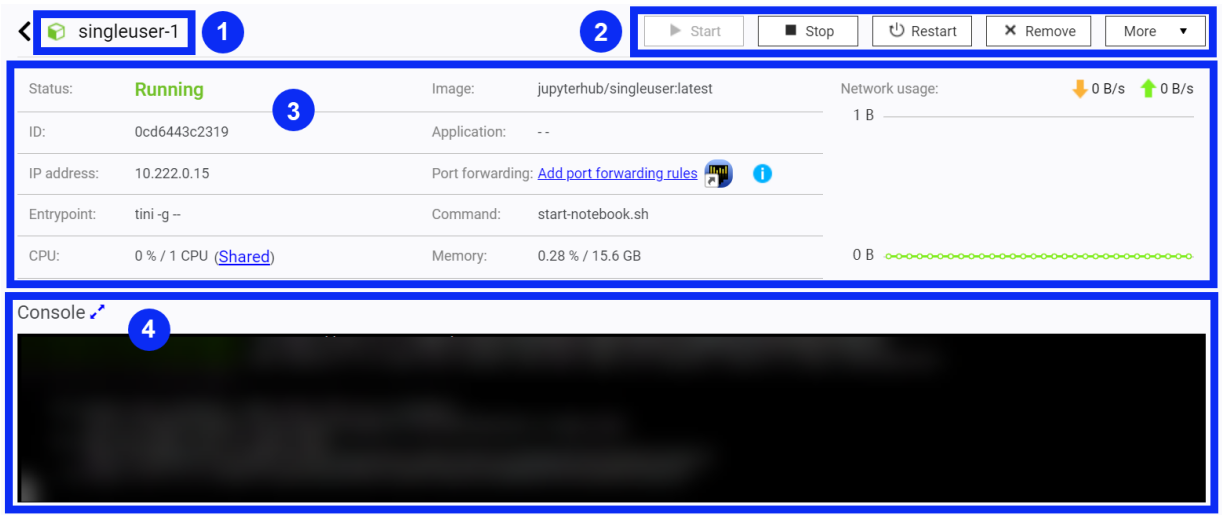


You can perform the following tasks on the **Overview** screen.

Task	Possible User Actions
Collapse or expand the **Overview** dashboard	Click ^ or v.
Select a container list	Click one of the following: • **All**: Displays a list of all containers on Container Station • **Running**: Displays only running containers • **Stopped**: Displays only stopped containers
Manage one or several containers	There are several ways to perform an action on a container. • On the container information screen, click a container name and then click an action button. For details, see Viewing the Container Information. • In the **Actions** column, click a button. • On the **Overview** or **Container** screen, select one or more containers and then click a button above the list. For details, see Managing Containers.

Viewing the Container Information

The container information screen has four main areas.



Label	Area	Description
1	Container name	Displays the container name
2	Action buttons	Displays the different buttons that can be used to perform an action on the container For details, see Managing Containers.

Label	Area	Description

3	Container details	Displays the following information:
		• **Status**: Displays one of the following statuses.
		  • Running
		  • Stopped
		  • Paused
		  • Created
		  • Dead
		  • Restarting
		  • Removing
		• **ID**: Displays the container ID
		• **IP address**: Displays the IP address
		• **Entrypoint**: Displays the entrypoint instruction
		• **CPU**: Displays the percentage of CPU usage
		• **Image**: Displays the image name and version number
		• **Application**: Displays the project name specified in the `docker-compose.yml` file
		• **Port forwarding**: Displays the port forwarding information
		• **Command**: Displays the CMD instruction
		• **Memory**: Displays the percentage of RAM usage
		Note
		Depending on the container settings, some fields may be empty.

4	Console or Logs	Displays either the command line terminal or the container logs depending on the container settings. The console is visible if you enabled **Allocate interactive and tty processes for the container** when you created the container. Otherwise, Container Station displays the logs. **Tip** Click to open the terminal on a new tab or window.

1. Select a method for viewing the container list.
   - On the menu, click **Overview**.
   - On the menu, click **Container**.

The list of available containers displays.

2. Click a container name.
   The container information screen displays.

Performing Actions on a Container

1. Select a method for viewing the container list.
   - On the menu, click **Overview**.
   - On the menu, click **Container**.

   The list of available containers displays.

2. Optional: Click a container name.
   The container information screen displays.

3. Perform an action on a container.

Task	Description	Steps

Start a container	Use this action to start a container.	• On the **Overview** or **Container screen**:
		  • In the **Actions** column, click ▶.
		  • Select one or more containers and then click **Start**.
		• On the container information screen:
		  • Click **Start**.

Stop a container	Use this action to stop all processes on a running container.
	When a container is not in use, it remains on the list unless removed.
		• On the **Overview** or **Container** screen:
		  • In the **Actions** column, click ■.
		  • Select one or more containers and then click **Stop**.
		• On the container information screen:
		  • Click **Stop**.

Restart a container	Use this action to restart a container.
	When a container becomes unresponsive, you can manually restart it.
	Note
	This action is not available for all containers.
		• On the **Overview** or **Container** screen:
		  • In the **Actions** column, click ⏻.
		  • Select one or more containers and then click **Restart**.
		• On the container information screen:
		  • Click **Restart**.

Task	Description	Steps

Remove a container	Use this action to remove a container.	• On the **Overview** or **Container** screen:
		  • In the **Actions** column, click ✕.
		  • Select one or more containers and then click **Remove**.
		• On the container information screen:
		  • Click **Remove**.

Pause a container	Use this action to suspend all processes on a running container. When you pause a container, you can stop the service without losing some settings, such as the IP address.	• On the **Overview** or **Container** screen:
		  • Select one or more containers and then click **More** > **Pause** .
		• On the container information screen:
		  • Click **More** > **Pause** .

Resume a container	Use this action to resume all processes on a paused container.	• On the **Overview** or **Container** screen:
		  • Select one or more containers and then click **More** > **Resume** .
		• On the container information screen:
		  • Click **More** > **Resume** .

Kill a container	Use this action to abruptly stop a container and end all processes.	• On the **Overview** or **Container** screen:
		  • Select one or more containers and then click **More** > **Kill** .
		• On the container information screen:
		  • Click **More** > **Kill** .

Edit the container settings	Use this action to modify the container settings.	On the container information screen: **a.** Modify the container settings, as needed. **b.** Click **Update**. Container Station saves the changes. For more details on the available container settings, see Editing the Container Settings.

Task	Description	Steps
Duplicate a container	Use this action to a create a new container based on an existing container.	**Note** This action is only possible from the container information screen. **a.** Click **More** > **Duplicate** . The **Create Container** wizard opens. **b.** Modify or keep the default settings. **c.** Click **Next**. The **Summary** screen displays. **d.** Review the container settings and then click **Create**. Container Station creates the container.
Create an image from a container	Use this action to create a new image from an existing container.	**Note** This action is only possible from the container information screen. • Click **More** > **Create image** . The **Create Image from Container** window opens. • Specify the image name. • Specify the image version. • Click **Create image**.
Execute a command from the terminal	Use this action to execute commands on a running container. The command line terminal allows you to more easily check logs and statuses, and perform actions without using a web server.	• On the **Overview** or **Container** screen: 1. In the **Actions** column, click >_ . 2. Type the command. 3. Click **Connect**.

Container Station performs the specified action.

Editing the Container Settings

1. Select a method for viewing the container list.
   - On the menu, click **Overview**.
   - On the menu, click **Container**.

   The list of available containers displays.
2. Click a container name.
   The container information screen displays.
3. Go to **More** > **Edit** .
   The **Edit Container** window opens.

4. Modify any of the following settings.

Field	Possible User Actions
Name	Specify the container name. **Note** The name must have 2 to 64 characters, starting with a letter or number, and it can only contain the following characters: • Letters: Upper case (A to Z) and lower case (a to z) • Numbers: 0 to 9 • Special characters: hyphen (-), underscore (_), or period (.)
Restart policy	Select one of the following for the restart policy options. • **None**: The container does not automatically restart. • **On failure**: The container automatically restarts only if it exits due to an error. • **Always**: The container automatically restarts even if it was previously stopped. • **Unless stopped**: The container does not automatically restart if it was previously stopped. **Note** The restart policy determines whether or not a container also restarts when the server or application restarts.
CPU	Allocate CPU resources for the container. **a.** Click **Specify CPU Resources**. The **CPU** window opens. **b.** Select a method. • **Shared**: The threads can be shared with other services. • **Dedicated**: The current service occupies the threads until you modify the settings. **c.** Select the number of cores and threads. **Note** Click **Select All** to allocate all the cores and threads on the list. **d.** Click **Apply**. **Important** You cannot configure shared and dedicated CPU resources for devices supporting less than four cores and eight threads.
Memory	Select whether the memory is unlimited or limited. If you select **Limited**, specify the memory size.
Reserved memory	Select whether the reserved memory is unlimited or limited. If you select **Limited**, specify the reserved memory size.

Field	Possible User Actions
Connected networks	Connect a network to the container. **Tip** While creating a network you can only select one network connection. After container creation, you can add multiple network connections. **a.** Click **Connect**. The **Network Connection** window appears. **b.** Select a network. **c.** Select a virtual switch from either the virtual switch or Docker network list. **d.** Select **Use static IP**. **e.** Specify a fixed IP address. **f.** Click **Connect**. **Tip** To disconnect from a virtual switch, click .

5. Click **Update**.
   Container Station saves the changes.

Managing Images

The **Images** screen allows you to pull and remove images, and create containers.

1. On the menu, click **Images**.
   The list of available images displays.
2. Perform any of the following tasks.

Task	Description	Action

Pull an image	Use this action to download a copy of an image into Container Station.
	When you pull images before creating a container, Container Station displays the image details which you can use to configure a container.
	
	Note
	Container Station uses the Docker Hub registry.
		a. Click **Pull**.
		
		b. Type the image name.
		Image names must start and end with a letter or number, and can contain between 1 and 128 characters of the following types:
		• Letters: a–z
		• Numbers: 0–9
		• Special characters:
		  • Hyphen (-)
		  • Underscore (_)
		  • Period (.)
		  • Forward slash (/)
		  • Colon (:)
		
		Note
		Using consecutive special characters in the image name is not allowed.
		
		c. Specify the image version.
		Image versions must start with a letter, number, or underscore (_), and can contain between 1 and 128 characters of the following types:
		• Letters: A–Z, a–z
		• Numbers: 0–9
		• Special characters:
		  • Hyphen (-)
		  • Underscore (_)
		  • Period (.)
		
		d. Optional: Enable **Set to default**.
		
		e. Click **Pull**.

Remove an image	Use this action to remove an image. **Note** Removing an image from the Container Station list does not remove the original image from Docker Hub.	• To remove an image, click ✕ in the **Actions** column. • To remove multiple images, select the images and then click **Remove**.

Task	Description	Action
Create a container from an image	Use this action to create a container using the selected image.	Click + in the **Actions** column and then use the **Create Container** wizard. For details, see Container Creation.

Container Station performs the specified action.

Managing Volumes

The **Volumes** screen allows you to create volumes, prune all unused volumes, remove volumes from the list, and identify which containers are using specific volumes.

1. On the menu, click **Volumes**.
   The list of available volumes displays.
2. Perform any of the following tasks.

Task	Action
Create a new volume	**a.** Click **Create**. The **Create Volume** window opens. **b.** Specify the volume name. **c.** Click **Create**. Container Station creates a new volume.
View a list of containers using a specific volume	Identify a volume in the list and then click .
Remove all unused volumes	Click **Prune**.
Remove a specific volume **Note** You can only remove volumes that are not currently in use.	• To remove a volume, click × in the **Actions** column. • To remove multiple volumes, select the volumes and then click **Remove**.

Container Station performs the specified action.

Managing Logs

Container Station logs actions that are performed inside the application. You can view and filter the logs, and download a copy in a CSV file.

- Perform any of the following tasks.

Task	Possible User Actions
Filter the logs	Click beside a column heading and then perform any of the following steps, as needed. • Deselect the information that you want to hide. • Specify the start and/or end dates. • Type a keyword.
Clear any existing filters to display all logs	Click **Reset Filter**.

Task	Possible User Actions
Download the logs as a CSV file	Click **Download**.

13. HA Manager

HA Manager provides high availability management for pairs of QNAP devices running QNE to maximize service uptime.

Note
HA Manager currently only supports QuCPE devices running QNE.

Installing HA Manager

1. Log on to QNE as an administrator.
2. Open Application Store, and then click  .
   A search box appears.
3. Enter `HA Manager`.
   The HA Manager application appears in the search results.
4. Click **Install**.
   The installation window appears.
5. Click **OK**.

QNE installs HA Manager.

High Availability (HA)

High availability builds redundancy in a system in order to reduce operational downtime whenever failure occurs. HA Manager provides this service by connecting two identical devices—an active device that runs services, and a standby device that functions as a real-time copy of the active device. When the active device fails, the standby device can automatically take over service operations with minimal disruption.

HA Requirements

To set up HA for your QNE devices, you must prepare the following items.

- Two QNE devices with the following identical specifications and components:
  - Device model

Note
HA Manager currently supports QuCPE devices only.

  - Firmware version
  - CPU model
  - Memory capacity
  - Application disk specifications
  - Network module model
  - Number of power supply units
  - At least one 10 Gigabit or greater network port

- One 10 Gigabit or greater network cable

Note

- This cable connects the HA link ports between the QNE devices.
- Both QNE devices must have the same HA link port number.
- The HA link allows data detection and synchronization from the active node to the standby node.

- Two network cables

Note

- These cables connect the management port of each QNE device to the network. The management port allows you to access and manage the active node and standby node devices.
- For each device, you must configure a static IP address for the management port. You can configure the static IP addresses during HA configuration.
- Both QNE devices must have the same management port number.

- Optional: Virtual IP address

Note
Setting up a virtual IP address allows you to maintain a constant connection to the active node no matter which device becomes the active node after a failover or switchover.

Configuring HA

Note
To configure HA between two devices, the devices must meet certain minimum requirements. For details, see HA Requirements.

1. Determine which of the two devices to set up as the active node.
2. Power on the active and standby node devices.
3. Connect the active and standby node devices to the same network.
4. Initialize the active node device.
5. Optional: Initialize the standby node device.

Tip
You can also let HA Manager initialize the standby node device later.

6. Prepare the pairing process.
   a. Log on to QNE on the active node.
   b. Install HA Manager.
   For details, see Installing HA Manager.
   c. Open HA Manager.
   The **Welcome to High Availability (HA) Manager** screen appears.

d. Click **Start**.
The **HA Requirements** screen appears.

e. Read the HA requirements.

f. Click **Next**.
The **Configure the Standby Node Device** screen appears.

g. Enter the IP address of the standby node device using one of the following methods:

- Type in the IP address of the standby node device.
- Click  and select the standby node device from the network list.

h. Answer the following question and follow the relevant steps.

Is the Standby Node Device Initialized?	User Action
Yes	**1.** Enter a username and password of the standby node device. **2.** Click **Next**.
No	**1.** Leave the username and password fields blank. **2.** Click **Next**. A confirmation window for initializing the standby node device appears. **3.** Click **Yes**. The **Initialize the Standby Node Device** screen appears. **4.** Enter a hostname for the standby node device. **5.** Click **Start**. A confirmation window appears. **6.** Click **Confirm**. The system initializes the standby node device. This process may take some time. **7.** Click **Next**.

The system checks whether HA Manager is installed on the standby node device.
The system installs HA Manager on the standby node device if the application is not yet installed. This process may take some time.

i. Click **Next**.
The **HA Device Pairing** screen appears.

7. Pair the active and standby node devices.

a. Check the specification comparison between the active and standby node devices.

b. Optional: Click **Back** and make adjustments and/or replacements to ensure specification consistency between the two devices.

c. Click **Next**.

The **HA Link Configuration** screen appears.

8. Set up the network.

a. Select a minimum 10 Gigabit network port on each device as the HA link port.

Important
Both devices must use the same port number for the HA link.

b. Connect the HA link port on the active node device to the HA link port on the standby node device with a minimum 10 Gigabit network cable.

c. Select the connected HA link ports.

d. Click **Next**.
The **Management Port Configuration** screen appears.

e. Select a port on each device as the management port.

Important

- The management port on each device must be a native port, and must be configured with a static IP address.
- Both devices must use the same management port number.

f. Connect the management port on the active node device to the network (if not already connected).

g. Connect the management port on the standby node device to the network (if not already connected).

h. Select the connected management ports.

i. Click the active node management port to configure a static IP address for the port.

j. Click the standby node management port to configure a static IP address for the port.

k. Click **Next**.
The **Configure Virtual IP Address** screen appears.

l. Optional: Select **Enable virtual IP address** and enter your virtual IP address and subnet mask.

Note
Setting up a virtual IP address allows you to maintain a constant connection to the active node no matter which device becomes the active node after a failover or switchover.

m. Click **Apply** to enable the virtual IP address, or click **Cancel** to set it up later.
The **HA Settings Summary** screen appears.

9. Create the HA environment.

a. Optional: Edit the standby node hostname.

b. Optional: Enter a description for each device.

c. Optional: Edit the HA group ID.

Note
This field cannot be blank.

d. Click **Create** after confirming the HA settings summary.
A warning message appears.

e. Select the checkbox to acknowledge all data on the standby node device will be deleted.

f. Click **Yes** to start creating the HA environment.

Important
Ensure power stability during the process.

g. Wait for HA Manager to reinitialize the standby node device, install applications, and sync the system and application configurations between the node devices.
A confirmation message appears when the configuration is complete.

10. Click **OK**.

HA Manager configures HA between the two devices.

You can configure additional settings in **HA Settings** > **Policies** .

Removing HA Configuration

To replace a node device, you must first remove the HA configuration.

You can initiate HA configuration removal from either node device.

Note
If you only want to reconfigure a device or perform device maintenance, QNAP recommends shutting down the device without removing the HA configuration. For details, see Shutting Down Node Devices.

1. Log on to QNE on the active or standby node.
2. Open HA Manager.
3. Go to **HA Settings** > **HA Maintenance** .
4. Click **Remove HA Configuration**.
The **Remove HA Configuration** screen appears.
5. Select one of the following:
   - **Reset network settings on standby node "[HOSTNAME]"**
   - **Reinitialize standby node "[HOSTNAME]"**

Warning
Reinitializing the standby node will delete all existing data on the node.

6. Enter the password for the standby node device.
7. Select the checkbox to acknowledge the warning.
8. Click **OK**.

HA Manager removes the HA configuration between the node devices.

HA Status

On the **Overview** screen, the icon between the two node devices indicates their current HA status. Hover over the icon to see the specific condition and recommended action.

Tip
You can also monitor the HA status and logs on AMIZ Cloud by enabling cloud management mode on both node devices in the myQNAPcloud app. To monitor the HA status on AMIZ Cloud, go to **HA Groups** and locate the HA group ID for your node devices.

Icon	Status	Condition	Recommended Action
	Normal	HA configuration status is normal.	-
	Action in progress	The following data is being synced from the active node to the standby node: • System and application configurations • Application volume data (such as virtual machine app data, container app data, and remote mount cache data) • Software component and application updates	Wait until the status changes to perform any new actions.
		HA switchover in progress.	
		Removing HA configuration.	
	Warning	Management port interruption.	Check the management port connections.
		Hardware component failure on a node device.	Check the device information to evaluate whether a device switchover is required.
	Error	HA link interruption.	Check the HA link connection.
		Unable to detect peer node.	Check the HA link and management port connections.
		Split-brain condition detected.	Click **Recover** to select which device to configure as the active node. For details, see Split-Brain.
		An unexpected error occurred during data synchronization.	Click **Recover** to reinitialize the standby node device.
		An unexpected error occurred.	Contact QNAP Customer Service. **Note** You can download debug reports from HA Manager and attach them in your support ticket. For details, see Reporting Issues.

Maintaining HA and Device Information

This section provides steps for editing, viewing, or configuring a virtual IP address, device information, notifications, and event logs.

Some actions are only available on the active node device.

All notification rules, including notification rules for applications other than HA Manager, are synced from the active node to the standby node. QuLog Center settings are also synced from the active node to the standby node. For these reasons, although you can view notification history and monitor event logs on the standby node, you cannot modify the notification rules or QuLog Center settings from the standby node.

Action	Availability on Node Device		User Action
	Active Node	Standby Node	
Adding a virtual IP address	Yes	No	1. In HA Manager, go to **HA Settings** > **HA Maintenance** . 2. Click **Virtual IP address is not configured.**
Editing the virtual IP address	Yes	No	1. In HA Manager, go to **HA Settings** > **HA Maintenance** . 2. Click ✎ next to **Active Node**.
Editing device descriptions	Yes	No	1. In HA Manager, go to **HA Settings** > **HA Maintenance** . 2. Click ✎ under the active node hostname or the standby node hostname.
Editing the HA group ID	Yes	No	1. In HA Manager, go to **HA Settings** > **HA Maintenance** . 2. Click ✎ next to the HA group ID field.
Viewing HA Manager notification history	Yes	Yes	1. In HA Manager, go to **HA Settings** > **Notification Settings** 2. Click **View notification history**.
Configuring HA Manager notification rules	Yes	No	1. In HA Manager, go to **HA Settings** > **Notification Settings** 2. Click **Configure Notification Rule**. The Notification Center application opens. For details, see "Notification Center" in the QNE User Guide.
Monitoring HA Manager event logs	Yes	Yes	In HA Manager, go to **Event Logs**.
Managing HA Manager event log settings	Yes	Can view, cannot modify	• Active node: a. Open QuLog Center from the QNE desktop. The QuLog Center application opens. • Standby node: a. In HA Manager, go to **Event Logs**. b. Click **QuLog Center**. The QuLog Center application opens. For details, see "QuLog Center" in the QNE User Guide.

Failover and Switchover

In an HA configuration, the standby node device is configured to quickly take over all services when the active node device fails. This takeover process is called a failover when it is automatic, and a switchover when it is performed manually.

After a failover or switchover, the standby node device becomes the new active node, and the failed active node device becomes the new standby node, allowing the failed device to be repaired while its services continue to operate on the new active node with minimal interruption.

Note

- The amount of time it takes for services on the original active node to resume on the new active node depends on what applications were running on the original active node and the amount of resources they used. For example, if you were running VMs in Virtualization Station, the takeover process would require more time.
- System configuration data or application data may be lost if the takeover process occurs during data synchronization.

Tip
If you are running VMs in Virtualization Station, QNAP recommends taking snapshots of the VMs before performing a switchover. This protects your data and minimizes data loss during the takeover process.

Enabling Automatic Failover

Automatic failover can only be enabled from the active node.

1. Log on to QNE on the active node.
2. Open HA Manager.
3. Go to **HA Settings** > **Policies** .
4. Select **Enable automatic failover**.
5. Select one or more **Failover Events**, any of which would trigger failover.
6. Optional: Select **Enable automatic failback**.

Note
This setting allows the original active node device to automatically resume the active node role once it has been repaired after a failover.

7. Click **Apply**.

HA Manager enables automatic failover.

Performing Manual Switchover

Manual switchover can be initiated from one of the node devices under different conditions, but is disabled during certain system processes.

Condition	Manual Switchover Available
Active node device hardware failure in any of the following components: • Loss in redundant power supply **Note** This only applies to device models that have a redundant power supply. • Failure of system fan module • Failure of CPU fan • Access denied to application volume • Errors related to disk health	Yes
The standby node is unable to detect the active node.	Yes, but can only initiate from the standby node
The active node is unable to detect the standby node.	No
The system is setting up the initial HA configuration between the two devices.	No
The system is updating the firmware on both devices.	No
The system is syncing data between the node devices.	Yes, but may cause data loss or unexpected errors
All other situations	Yes

1. Log on to QNE on the active or standby node.
2. Open HA Manager.
3. Go to **HA Settings** > **HA Maintenance** .
4. Click **Switchover**.
   A warning message appears.
5. Click **Yes**.

HA Manager begins the switchover process.

Split-Brain

Split-brain is a condition in which both node devices have assumed the role of the active node.

One common scenario in which split-brain occurs is when the active and standby nodes experience network interruption during a failover. At the moment of network interruption, the standby node has assumed the active node role, but the original active node has not yet assumed the standby node role. After the network is restored, the system detects split-brain.

Automatic and manual methods of split-brain recovery are available.

Enabling Automatic Split-Brain Recovery

Automatic split-brain recovery allows the system to self-correct as soon as the condition is detected, minimizing the duration of service interruption.

Automatic split-brain recovery can only be enabled from the active node.

1. Log on to QNE on the active node.
2. Open HA Manager.
3. Go to **HA Settings** > **Policies** .
4. Select **Automatic recovery from split-brain**.
5. Select which node and condition to discard the changes that have occurred since split-brain.

Note
The selected node will become the standby node after recovery.

6. Click **Apply**.

HA Manager enables automatic split-brain recovery.

Performing Manual Split-Brain Recovery

When automatic split-brain recovery is disabled, and split-brain has been detected, the HA status icon on the **Overview** screen indicates an error on both the active and standby nodes, and a **Recover** button appears.

Because the data between the two devices are no longer synced after split-brain occurs, you may want to save and compare the data between the two devices, before deciding which device to configure as the active node.

1. Log on to QNE on one of the devices.
2. Open HA Manager.
3. Go to **Overview**.
4. Click **Recover**.
   The **Split-Brain Recovery** screen appears.
5. Answer the following question and follow the relevant steps.

Do you want to save device data?	User Action
No	**a.** Select which device to configure as the active node during recovery. **b.** Click **Enable Active Node**. Split-brain recovery begins.

Do you want to save device data?	User Action
Yes	**a.** Click **Remove HA Configuration**. The **Remove HA Configuration** screen appears. **b.** Select which device to reset network settings. **c.** Enter the password for the selected device. **d.** Select the checkbox to acknowledge the warning. **e.** Click **OK** to remove the HA configuration. **f.** Save the data on each device. **g.** Determine which device to configure as the active node. **h.** Open HA Manager on the active node desktop to reconfigure HA between the node devices. For details, see Configuring HA.

Node Device Operations

When an HA link has been configured between two QNE devices, certain operations on the devices become interdependent. These operations are performed automatically on both devices in a set procedure to ensure the HA configuration is correctly preserved.

Operation	Can Initiate from Node Device	
	Active Node	Standby Node
Shut down both devices	Yes	No
Restart both devices	Yes	Yes, when an installed or updated software component requires a system restart **Note** After login, a popup message appears with a button that allows you to restart the devices.
Update the firmware on both devices	Yes	No

Important
If you wish to perform these operations on only one device, you must remove the HA configuration first. For details, see Removing HA Configuration.

Shutting Down Node Devices

To shut down both devices in an HA configuration, you must initiate the process from the active node.

Note

- To ensure the devices resume their current node roles when starting the devices after the shutdown, do not disconnect the power supply during the shutdown process.
- To shut down a single device, you must first remove the HA configuration. For details, see Removing HA Configuration.

1. Log on to QNE on the active node.
2. On the QNE desktop, click **[USERNAME]**.
   A drop-down menu appears.
3. Click **Shutdown**.
   A confirmation message appears.
4. Click **Confirm**.
   a. The shutdown screen appears.
   b. The active node requests the standby node to shut down.
   c. The standby node shuts down.
   d. The active node confirms that the standby node has shut down.
   e. The active node shuts down.

Restarting Node Devices

To restart both devices in an HA configuration, you must initiate the process from the active node under most circumstances.

If an installed or updated software component requires a system restart, when you log in to either device, a popup message appears and asks you to restart the devices. In this scenario, you can initiate the restart process from either the active node or the standby node by clicking the corresponding button in the popup message.

Note

- To ensure the devices resume their current node roles after restart, do not disconnect the power supply during the restart process.
- To restart a single device, you must first remove the HA configuration. For details, see Removing HA Configuration.

1. Log on to QNE on the active node.
2. On the QNE desktop, click **[USERNAME]**.
   A drop-down menu appears.
3. Click **Restart**.
   A confirmation message appears.
4. Click **Confirm**.
   a. The restart screen appears.
   b. The active node requests the standby node to restart.
   c. The standby node restarts.
   d. The active node confirms that the standby node has restarted.
   e. The active node restarts.
   f. The active node reconnects with the standby node and checks the status of the standby node.

Note
If the active node is unable to check the status of the standby node before timeout, the system enters an error status. For details on resolving the error status, see HA Status.

g. The system reestablishes the HA link between the node devices.

Updating Node Device Firmware

To update the firmware on both devices in an HA configuration, you must initiate the process from the active node.

Note

- To ensure the devices resume their current node roles after the firmware update, do not disconnect the power supply during the update process.
- To update the firmware on a single device, you must first remove the HA configuration. For details, see Removing HA Configuration.

1. Log on to QNE on the active node.
2. Go to **Control Panel** > **System** > **System Update** > **Firmware Update** .
3. Click **Check for Update**.

Tip
You can also update the firmware manually. For details, see "Updating the Firmware Manually" in the QNE User Guide.

a. The active node copies the new firmware to the standby node.

b. The active node requests the standby node to perform a firmware update.

c. The HA link is severed and data synchronization is halted.

d. The standby node updates the device firmware and restarts.

Note
If the update process times out on the standby node, the firmware update is canceled on both devices and the HA link is reestablished.

e. The active node confirms the standby node has successfully updated the device firmware and restarted.

f. The active node updates the device firmware and restarts.

Note
If the update process times out on the active node, the firmware update is canceled on both devices and the HA link is reestablished.

g. The active and standby nodes reconnect and reestablish the HA link.

Reporting Issues

If HA Manager encounters any issues, you can download and submit debug reports from each node device to QNAP Customer Service.

The debug reports between the node devices differ depending on the HA status.

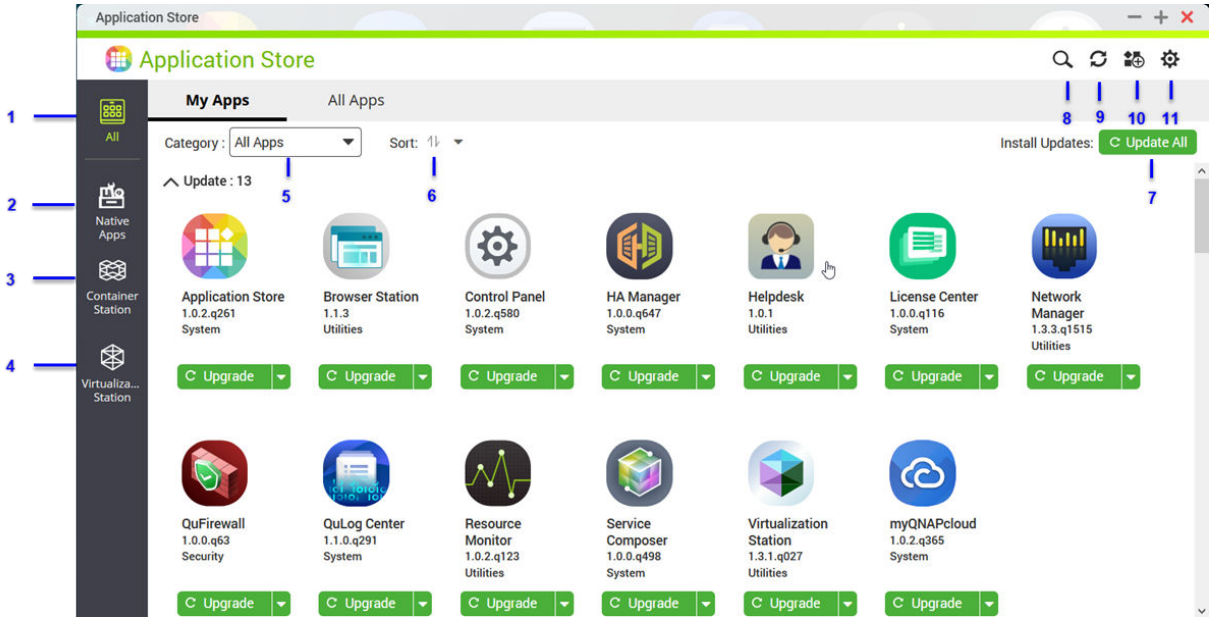
HA Status	Debug Report from Active Node	Debug Report from Standby Node
Normal	Contains information on both the active and standby nodes.	Contains information on the standby node only.
Unable to detect peer node	Contains information on the active node only.	Contains information on the standby node only.
Split-brain condition detected	Each debug report contains information on its own node only.	Under split-brain condition, there is no standby node.

1. Download the debug report from a node device.
   a. Log on to QNE on the device.
   b. Open HA Manager.
   c. Go to > **Debug Report** .
      The **Download Debug Report** window opens.
   d. Click **Download**.
      HA Manager downloads the debug report to your computer.
2. Optional: Download the debug report from the other node device.
3. Create a support ticket.
   a. Go to QNAP Customer Service.
   b. Log in to create a support ticket.
   c. Enter detailed information into all relevant fields.
   d. Upload the debug reports as attachments.
   e. Click **Send Message**.
      The support ticket is submitted. QNAP Customer Service will contact you via the email address you provided.

14. Application Store

Application Store is a digital distribution and management platform in QNE where you can browse, download, and manage apps and utilities developed for the QNAP device.

Navigation



No.	Elements	Possible User Actions
1	All	Click the tab to view all apps on this device.
2	Native Apps	Click the tab to view all QNAP developed apps for this operating system. You can view all installed QNAP apps on the device in the **My Apps** tab or all available QNAP apps in the **All Apps** tab.
3	Container Station	Click the tab to view and manage all container apps.
4	Virtualization Station	Click the tab to view and manage all virutalization apps.
5	Category	Click ˅ to sort apps by category type.
6	App sorting	Click ˅ and select an app sorting method.
7	Update all	Update all apps. For details, see Updating Apps.
8	Search	Specify keywords to search for apps. Application Store instantly displays search results based on specified keywords.
9	Refresh	Reload the data in Application Store to view the current status of your apps.
10	Manual installation	Manually install an app by uploading an installation package. For details, see Installing an App Manually.
11	Settings	Configure various Application Store settings.

App Installation

You can install apps automatically or manually in the Application Store to add functionality in QNE. You can also uninstall an unused app anytime.

Viewing App Information

You can browse apps and view their descriptions in the Application Store. This helps you decide whether to install or update an app.

1. Open Application Store.
2. Locate an app.
3. Click the app icon.
   Application Store displays the app information in a new window.
4. Perform one of the following actions.
   - View the app description
   - View the digital signature details
   - View the app changelog
   - Go to the QNAP forum
   - View the app tutorial
   - Download the app installation package

Installing an App from Application Store

Warning
QNAP recommends only installing apps from the Application Store or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.

Important

- Certain apps require activating a subscription or license before app installation. For details, see Licenses.
- Based on the app you choose to install, Application Store may display a confirmation message that provides more information and asks for your approval for installation. Certain apps also require you to specify the installation location. Read the message carefully before installing the app.

1. Open Application Store.
2. Locate an app.
3. Optional: Click the app icon to view the app information.
4. Select the app update frequency.
5. Click **Install**.

The app is installed.

Installing an App Manually

Warning

- QNAP recommends only installing apps from the Application Store or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.
- Application Store does not allow the installation of invalid apps, including apps with invalid digital signatures, apps not approved by Application Store, or from the Software Store. If Application Store detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.

Important
Certain apps require activating a subscription or license before app installation. You can go to the Software Store to purchase an app license or subscription. For details about activating an app license, see Licenses.

1. Open Application Store.
2. Click on the toolbar.
   The **Install Manually** window appears.
3. Click **Browse**.
4. Locate and select the installation package.
5. Click **Install**.
   A message appears.
6. Read the confirmation message.
7. Click **OK**.
   Application Store installs the app.

Uninstalling an App

Warning
Uninstalling an app also deletes the related user data.

1. Open Application Store.
2. Locate an app.
3. Click .
4. Select **Remove**.
   A confirmation message appears.
5. Click **Yes**.

App Management

The Application Store allows you to enable or disable an app, assign CPU resources to load-intensive apps, update apps, and configure app update settings.

Enabling or Disabling an App

You can enable or disable non-built-in apps in Application Store.

Note

- Disabling an app may affect the functionality of other apps.
- Disabling an app does not remove or uninstall the app.

1. Open Application Store.
2. Locate an app.
3. Perform one of the following actions.

Action	Steps
Enable the app	Click **Start**.
Disable the app	**a.** Click . **b.** Select **Stop**.

- After an app is enabled, its action button displays **Open**.
- After an app is disabled, its action button displays **Start**.

Assigning CPU Resources to Apps

Important
To use this feature, your device CPU must have a minimum of 4 cores and 8 threads.

QNE allows you to assign CPU threads to specific apps, providing flexibility in prioritizing CPU resources to load-intensive apps. You can view the allocated CPU thread statuses in the **Allocating CPU Resources** window.

For details about CPU thread statuses, see the table below.

Status	Definition
Dedicated	The CPU thread is dedicated to run a specified app and will not run any other apps.
Shared	The CPU thread is shared by several apps and runs multiple apps.
Idle	The CPU thread has not been allocated to any app.

1. Open Application Store.
2. Click .
   The action drop-down menu appears.
3. Click **Assign CPU**.

The **Allocate CPU Resources** window appears.

4. Select one or more CPU cores.
5. Select one or more CPU threads.
6. Optional: Click **Restore**.
   Application Store restores the assigned CPU resources of the app to default settings.
7. Click **Apply**.

Configuring App Update Settings

1. Open Application Store.
2. Click ⚙.
3. Go to **Update**.
4. Select **Perform the following action when updates are available** and then select one of the following options.

Option	Description
Send a notification	QNE sends notification messages when updates are available for your apps. You can click **Configure Notification Rule** to create rules in Notification Center. For details, see Notification Center.
Install all updates automatically	Application Store automatically installs all available updates for your apps. You can select how often Application Store should check for available updates.
Install all required updates automatically	Application Store automatically installs all required updates for your apps to ensure their functionality, compatibility, and data security. You can select how often Application Store should check for required updates.
Auto-update specified applications	Application Store automatically installs updates for specified apps. You can select the frequency that Application Store checks for available updates. You can select apps for automatic update.

5. Click **Apply**.

Updating Apps

When updates are available for an installed app, the app button status changes to **Upgrade**. You must perform required updates to ensure proper functionality, compatibility, and data security for your apps.

1. Open Application Store.
2. Select one of the following update methods:

Options	Steps
Update all apps	Click **Update All**.

Options	Steps
Update an app	**a.** Locate an app in the **Update** section. **b.** Click **Upgrade**.

Application Store begins updating an app or all apps.

15. Licenses

QNAP licenses enable users to gain access to certain advanced features or premium products. This chapter introduces important concepts and demonstrate essential tasks to help you start using QNAP licenses.

About QNAP Licenses

QNAP offers a wide variety of licenses. Some basic licenses are provided free of charge. You can purchase premium licenses to further enhance the functionality of your QNAP products. QNAP also provides multiple management portals, flexible subscription plans, and various activation options to meet your different needs.

License Types and Plans

The licensing mechanisms and available plans of QNAP licenses vary depending on corresponding software products. They can be divided into the following categories.

License Types

License Types	Description
Device-based	• Allows users to use a software product installed on hardware devices, such as applications. • Multi-seat licenses can be activated and used on multiple devices.
Floating	• Allows users to use a software product in the cloud or on a virtual platform, such as QuTScloud and applications in QuTScloud. • Can be activated and used on a limited number of devices at a time
User-based	• Allows a limited number of authorized users to access a web-based service, such as Qmiix.

License Plans

License Plans	Description
Subscription	Authorizes users to use a software product with a recurring monthly or annual fee
Perpetual	Authorizes users to use a software product indefinitely
One-time	Authorizes users to use a software product within a predefined period of time

Validity Period

The validity period of a QNAP subscription-based license starts from the date of purchase, not from the date of activation.

For example, if a user starts the subscription of an annual license on January 1, 2020, the next billing date will be January 1, 2021, regardless of the date of activation. If the user cancels the subscription, the license will still remain valid until January 1, 2021.

If the user unsubscribes from a license but subscribes to the same product later, the validity period and billing cycle will begin from the date of the new subscription.

License Portals and Utility

Portal	Description	URL
QNAP Software Store	The QNAP Software Store is a one-stop shop where you can purchase licenses for QNAP and QNAP-affiliated software.	https://software.qnap.com
QNAP License Center	The QNAP License Center allows you to monitor and manage licenses of applications running on your local device.	-
QNAP License Manager	QNAP License Manager is a portal that allows you and your organizations to remotely activate and manage licenses under your QNAP ID.	https://license.qnap.com
Old QNAP License Store	Users of QNE 4.3.4 (or earlier) can purchase licenses from this online store.	https://license2.qnap.com

Software Store

Software Store allows you to purchase licenses for applications. Through Software Store, you can perform the following actions.

- Purchase or upgrade licenses
- Manage your account information
- View purchased subscriptions
- Cancel your subscriptions
- Request a refund for your orders

License Center

License Center allows you to monitor and manage the licenses of your applications running on your local device. Through License Center, you can perform the following actions.

- Activate and deactivate licenses either online or offline
- Remove licenses from the local device
- Recover licenses if your device is reset, reinitialized, or restored to factory default
- Transfer licenses purchased from the old QNAP License Store to the new QNAP License Manager

License Manager

License Manager is a portal that allows you to manage all licenses under QNAP IDs and organizations. Through License Manager, you can perform the following actions.

- View details of your licenses
- Activate and deactivate licenses
- Assign a user-based license to a QNAP ID

Important
To remotely activate or deactivate licenses, you must enable myQNAPcloud Link on your QNAP device.

Buying a License Using QNAP ID

Before buying a license, ensure the following.

- The application is already installed on your device.
- You are signed in to myQNAPcloud.

1. Go to https://software.qnap.com.
2. Sign in with your QNAP ID.
3. Locate the product on the list, and then click **Buy** or **Subscribe Now**.
   The license details appear.
4. Select the item you want to buy, and then review the price.
5. Click **Checkout Now**.

Tip
You can also click **Add to Cart** and then continue shopping.

   The purchase summary page appears in your web browser.

6. Select a payment method.

Payment Method	User Action
Credit card	**a.** Specify your card information. **b.** Verify the items and the price on the order. **c.** Agree to QNAP terms and conditions. **d.** Click **Place Order**.
PayPal	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Pay with PayPal** PayPal authentication window appears. **d.** Specify your PayPal login credentials. **e.** Click **Next**. **f.** Follow PayPal instructions to complete the payment.
Google Pay	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Buy with Google Pay**. Google Pay authentication window appears. **d.** Follow Google Pay instructions to complete the payment.

After the payment, you can view order details in **My Orders** and manage your subscriptions in **My Subscriptions**.

You can activate your license right after the purchase or at a later time.

For details, see License Activation.

License Activation

You need to activate purchased licenses to access features provided by the license. You can activate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through Software Store are stored in your QNAP ID account. They can be accessed through both License Center and the QNAP License Manager website.
Using a license key	You can generate the 25-character license key after purchasing licenses through the QNAP Software Store. For details, see Generating a License Key. You can use license keys to activate licenses in License Center. For details, see Activating a License Using a License Key.
Using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. You can use product keys to activate licenses in License Center. For details, see Activating a License Using a Product Key or PAK.
Using a product authorization key (PAK)	The 24-character PAK is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. For details, see Activating a License Using a Product Key or PAK.
Offline	Use this method when the device is not connected to the internet. For details, see Activating a License Offline.

Activating a License Using QNAP ID

Before activating your license, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.
- You have signed in with your QNAP ID.

Users can activate their licenses using QNAP ID in either Qfinder Pro, License Center, or License Manager.

- Activate your license using one of the following methods.

Method	Steps
License Center	**a.** Open License Center. **b.** Go to **My Licenses**. **c.** Click **Activate License**. The **License Activation** window appears. **d.** Select **Activate with QNAP ID**. **e.** • In Stand-Alone Mode, click **Select License**. • In Cloud Management Mode, click **My QID License** or **Organization License**. **Tip** In Cloud Management Mode, you can choose to activate a license that belongs to your QNAP ID or your organization. **f.** Select a license from the list. **Tip** If you select a multi-seat license, you can specify the number of seats that you want to activate. **g.** Click **Add**. License Center activates the license. A confirmation message appears. **h.** Click **Close**. The license appears on the list of active licenses.
License Manager	**a.** Open your web browser. **b.** Go to https://license.qnap.com. **c.** Sign in with your QNAP ID. **d.** Locate a license from the license list. **e.** Click  . The **Activate License** window appears. **f.** Select **Online Activation**. **g.** Select a device. **h.** Specify your credentials on the device. **i.** Click **Allow**. A confirmation message appears. **j.** Click **OK**. License Manager activates the license. **k.** Click **Close**. The license appears on the list of active licenses.

Activating a License Using a License Key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID.

You can activate a license using a license key. After purchasing a license from QNAP Software Store, you can generate a license key from the License Manager website and apply the key in License Center. A license key contains 25 characters and always starts with the letter L.

For details, see Generating a License Key.

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
   The **License Activation** window appears.
4. Select **Activate with a License Key**.
5. Specify the key.
6. Read and agree to the terms of service.
7. Click **Verify Key**.
8. Verify the license information.
9. Optional: Specify the number of seats to activate.

Note
This option is only available for licenses that support multiple seats.

10. Click **Activate**.
    The license is activated.
    A confirmation message appears.
11. Click **Close**.
    The license appears on the list of active licenses.

Generating a License Key

1. Open your web browser.
2. Go to https://license.qnap.com.
3. Sign in with your QNAP ID.
4. From the list of licenses, select the license you want to generate a key for.
5. Click .
   The **Activate License** window appears.
6. Select **License Key**.
   License Manager generates the license key.

Tip
Click **Renew License Key** to generate a new key.

> This renews your license key and protects you from any unauthorized access to your existing license key.

7. Hover the mouse pointer over the license key and click  .
   Your system copies the license.
8. Click **Done**.

The copied license key can be pasted later for license activation.

Activating a License Using a Product Key or PAK

Before activating a license using a product key or a product authorization key (PAK), ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

You can activate a license with a product key or PAK. You may find a product key printed on a physical copy of your product. A product key contains 25 characters and always starts with the letter P.

On the other hand, you may obtain a product authorization key (PAK) if you purchase a license from the old QNAP License Store. A PAK contains 24 digits of random numbers.

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
4. The **License Activation** window appears.
5. Select **Activate with a Product Key or PAK**.
6. Specify the key.
7. Read and agree to the terms of service.
8. Click **Verify Key**.
9. Verify the license information.
10. Click **Activate**.
    The license is activated.
    A confirmation message appears.
11. Click **Close**.
    The license appears on the list of active licenses.

Activating a License Offline

You can activate your license offline if your QNAP device is not connected to the Internet. You first need to generate a device identity file (DIF) from Qfinder Pro or from License Center on your device and then upload the DIF to License Manager in exchange for the license install file (LIF). You can then activate the license using the LIF in Qfinder Pro or in License Center on your device.

1. Choose one of the following methods.

Methods	User Action
Offline activation using Qfinder Pro	Qfinder Pro allows you to discover QNAP devices on your local network. **a.** Open Qfinder Pro on your computer. **Tip** You can download Qfinder Pro from the QNAP website. **b.** Select your device from the list. **c.** Right-click the device and then select **License Activation**. **d.** Specify your username and password. The **License Activation** window appears. **e.** Select **Offline Activation**.
Offline activation using License Center	**a.** Log in to your QNAP device. **b.** Open License Center. **c.** Go to **My Licenses**. **d.** Click **Activate License**. The **License Activation** window appears. **e.** Select **Offline Activation**.

2. Read and agree to the Terms of Service.
3. Click **Generate Device Identity File**.
   Qfinder Pro or License Center downloads the device identity file (DIF) to your computer.
4. Read the instructions and click **Go to License Manager**.
   Your web browser opens the **QNAP License Manager** website.
5. Sign in with your QNAP ID.
6. From the list of licenses, select the license you want to activate.
7. Click **(Upload Device Identity File)**.
   The **Activate License** window appears.
8. Click **Browse**.
   The file browser appears.
9. Locate and select the DIF from your computer.
10. Click **Upload**.
    A confirmation message appears.
11. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
12. Click **Done**.
13. Go back to Qfinder Pro or License Center.

14. In the **License Activation** window, click **Upload License File**.
15. Click **Browse**.
    The file browser appears.
16. Locate and select the LIF from your computer.
17. Click **Import**.
    Qfinder Pro or License Center uploads the LIF and displays the license summary.
18. Click **Activate**.
    The license appears on the list of active licenses.

License Deactivation

You can deactivate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website To deactivate this type of license, see Deactivating a License Using QNAP ID.
Offline	Use this method when the device is not connected to the internet. For details, see Deactivating a License Offline.

Deactivating a License Using QNAP ID

Before deactivating your license, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can deactivate their licenses using QNAP ID in either License Center or License Manager.

- Deactivate your license using one of the following methods.

Method	Steps
License Center	**a.** Open License Center. **b.** Go to **My Licenses**. **c.** Identify the license you want to deactivate, and then click  . The **License Deactivation** window appears. **d.** Select **Use QNAP ID**. **e.** Read and acknowledge the warning. **f.** Click **Deactivate**. A confirmation message appears. **g.** Click **Close**. License Center deactivates the license and removes the license from the list of active licenses.

Method	Steps
License Manager	**a.** Open your web browser. **b.** Go to https://license.qnap.com. **c.** Sign in with your QNAP ID. **d.** From the list of licenses, select the license you want to deactivate. **e.** Click . The **Deactivate License** window appears. **f.** Read and acknowledge the warning. **g.** Click **Deactivate**. License Center deactivates the license. A confirmation message appears. **h.** Click **Close**. License Center removes the license from the list of active licenses.

Deactivating a License Offline

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to deactivate, and then click .
   The **License Deactivation** window appears.
4. Select **Offline Deactivation**.
5. Read and acknowledge the warning.
6. Read the instructions, and then click **Generate License Uninstall File**.
   License Center downloads the license uninstall file (LUF) to your computer.
7. Open your web browser.
8. Go to https://license.qnap.com.
9. Sign in with your QNAP ID.
10. From the list of licenses, select the license you want to deactivate.
11. Under **Advanced Options**, click .
    The **Deactivate License** window appears.
12. Read and agree to the terms.
13. Click **Offline Deactivation**.
14. Click **Browse**.
    The file browser appears.
15. Locate and select the LUF from your computer.
16. Click **Upload**.

QNAP License Manager deactivates the license.
A confirmation message appears.

17. Click **Done**.

License Extension

License Center will notify you soon before any of your subscription-based licenses expire. The exact dates vary depending on the type of your licenses (ranging from one week to one month before the expiration date). You can extend your QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through License Center or Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website. If you have an existing valid, unused subscription-based license in License Center, you can use this to extend your expiring license. For details, see Extending a License Using QNAP ID.
Offline using an unused license	If you have a valid, unused subscription-based license and your device is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using an Unused License.
Offline using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you have a valid, unused product key for a subscription-based license, and your device is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using a Product Key.

Extending a License Using QNAP ID

Before extending licenses, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.
- You have an existing valid, unused license.

Note
Subscription-based licenses will be automatically renewed in License Manager. You cannot manually extend a subscription-based license.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .

Tip
If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

4. Select an unused license.

Warning
License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

5. Click **Extend**.
   License Center extends the license.
   A confirmation message appears.
6. Click **Close**.

Extending a License Offline Using an Unused License

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .

Tip
If a license is about to expire, its status is `Expires soon`.

   The **License Extension** window appears.

4. Select **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
   License Center downloads the device identity file (DIF) file to your computer.
8. Read and agree to the terms of service.
9. Click **Next**.
10. Read the instructions, and then click **Go to License Manager**.
    Your web browser opens the QNAP License Manager website.
11. Sign in with your QNAP ID.
12. Go to **My Licenses**.
13. From the list of licenses, select the license you want to activate.
14. In the table below, click **Activation and Installation**.
    The license activation details appear.
15. Click **Extend**.
    The **Extend License** window appears.
16. Select **Use an unused license**, and then click **Next**.
    The list of unused licenses appears.
17. Select an unused license.

Warning
License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

18. Click **Next**.
19. Click **Browse**.
    The file browser appears.
20. Locate and select the DIF from your computer.
21. Click **Upload**.
    A confirmation message appears.
22. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
23. Click **Done**.
24. Go back to License Center.
25. In the **License Extension** window, click **Next**.
26. Click **Browse Files**.
    The file browser appears.
27. Locate and select the LIF from your computer.
28. Click **Next**.
    License Center uploads the LIF and displays the license summary.
29. Click **Extend**.
    A confirmation message appears.
30. Click **Close**.
    The license appears on the list of active licenses.

Extending a License Offline Using a Product Key

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .

> **Tip**
> If a license is about to expire, its status is `Expires soon`.

The **License Extension** window appears.

4. Click **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
   A notification message appears.
8. Click **Download**.
   License Center downloads the device identity file (DIF) file to your computer.
9. Read and agree to the terms of service.

10. Click **Next**.
11. Read the instructions, and then click **Go to License Manager**.
    Your web browser opens the QNAP License Manager website.
12. Sign in with your QNAP ID.
13. Go to **My Licenses**.
14. From the list of licenses, select the license you want to activate.
15. In the table below, click **Activation and Installation**.
    The license activation details appear.
16. Click **Extend**.
    The **Extend License** window appears.
17. Select **Use a product key**, and then click **Next**.
18. Specify the product key.
19. Click **Next**.
    A confirmation message appears.
20. Click **Download**.
    QNAP License Manager downloads the license install file (LIF) to your computer.
21. Click **Done**.
22. Go back to License Center.
23. In the **License Extension** window, click **Next**.
24. Click **Browse Files**.
    The file browser appears.
25. Locate and select the LIF from your computer.
26. Click **Next**.
    License Center uploads the LIF and displays the license summary.
27. Click **Extend**.
    A confirmation message appears.
28. Click **Close**.
    The license appears on the list of active licenses.

Upgrading a License

Before upgrading a license, ensure the following.

- The application is already installed on your device.
- You are signed in to myQNAPcloud.

Users can upgrade their existing basic licenses to premium licenses to gain access to advanced features.

1. Open your web browser.
2. Go to https://software.qnap.com.

3. Click your account name and select **MY ACCOUNT**.
4. Click **Upgrade Plans**.
   A list of upgradable subscriptions is displayed.
5. From the list of subscriptions, find the license you want to upgrade and click **Upgrade**.
   The **Current Plan** window appears.
6. From the list of upgrade plans, select an upgrade and click **Add to Cart**.
7. Click  .
8. Click **GO TO CHECKOUT**.
9. Select a payment method.

Payment Method	User Action
Credit card	**a.** Specify your card information. **b.** Verify the items and the price on the order. **c.** Agree to QNAP terms and conditions. **d.** Click **Place Order**.
PayPal	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Pay with PayPal** PayPal authentication window appears. **d.** Specify your PayPal login credentials. **e.** Click **Next**. **f.** Follow PayPal instructions to complete the payment.
Google Pay	**a.** Verify the items and the price on the order. **b.** Agree to QNAP terms and conditions. **c.** Click **Buy with Google Pay**. Google Pay authentication window appears. **d.** Follow Google Pay instructions to complete the payment.

10. Apply the license upgrade to your QNAP device.
    a. Open your web browser.
    b. Go to https://license.qnap.com.
    c. Sign in with your QNAP ID.
    d. Locate the license from the license list.
    e. Click  .
    The **Activate Upgraded License** window appears.

f. Select **Online Activation**

g. Click **Next**.

h. Specify your credentials on the device.

i. Click **Allow**.
A confirmation message appears.

j. Click **Close**.

The upgraded license is activated.

Viewing License Information

1. Open your web browser.
2. Go to https://license.qnap.com.
3. Sign in with your QNAP ID.
4. View the license information using one of the following modes.

Viewing Mode	User Actions
List by Device	This mode displays all the activated licenses on each device. This allows you to quickly view and manage your licenses on a specific device. • Click a device and then click **Device Details** to view the details of the selected device. • Click a device and then click **Activation and Installation** to view the details of your licenses. You can also activate or deactivate licenses.
List by License	This mode displays your purchased licenses and their details, including available seats, license types, validity period, and status. • Click a license and then click **License Details** to view the details. • Click a license and then click **Activation and Installation** to view the details. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file. • Click a license and then click **Usage Record** to view the history of the selected license.
List by Product	This mode displays your purchased licenses for each product. This allows you to view and manage all related licenses designed for the same product. • Click a product to view the details of your licenses. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file.

Recovering Licenses

Before recovering licenses, ensure that your device is connected to the internet.

1. Open License Center.
2. Go to **Recover Licenses**.

3. Click **Get Started**.
   The **License Recovery** dialog box appears.
4. Read and agree to the terms of service.
5. Click **Recovery**.
   License Center automatically recovers all available licenses for applications installed on your devices.

Transferring a License to the New QNAP License Server

This task only applies to existing licenses that have been activated using PAK.

Before transferring licenses, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to transfer, and then click .
   A confirmation message appears.
4. Read the terms of service, and then click **Transfer & Activate**.

Warning
After you register a license with your current QNAP ID, it will no longer be transferable.

   License Center transfers the license.
   A confirmation message appears.
5. Optional: Click **QNAP License Manager** to review the license details.
6. Click **Close**.

Deleting a License

Before deleting a license, ensure that you have deactivated this license.

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to delete, and then click .
   A confirmation message appears.
4. Click **Yes**.
   License Center deletes the license.

Tip
If the license has not yet expired, the license will still be listed in the **License Activation** table.

16. QuLog Center

QuLog Center provides a centralized log management solution for local devices and remote devices. You can monitor and manage local logs on a local device, or set up your device as a remote log management center using QuLog Service. For details about QuLog Center concepts and terms, see the following table.

Terms	Definition
Event Log	The event log is a record of system events, such as system, security, and application notifications. Events are stored by the device operating system for administrators to diagnose system problems and troubleshoot issues.
Access Log	The access log is a detailed record of user access to applications and files on a device.
Local Device	The current device you are logged in.
QuLog Service	The QuLog Service is a remote log management service that allows you to centrally manage remote logs on the local device. The QuLog Service also allows you to send local device logs to a remote QuLog Center or to a Syslog Server.
Log Receiver	The local device that is the recipient of all remote device logs. The Log Receiver functions as the central log management platform for up to 500 remote devices.
Log Sender	A local device that sends logs to a remote QuLog Center on another device or to a Syslog Server.
Sender Device	A remote device that sends logs to the local Log Receiver.

Monitoring Logs

The **Overview** > **Event Log** and **Overview** > **Access Log** screens provide statistical graphics to help you visualize system log data and monitor device status.

Monitoring Event Logs

The **Overview** > **Event Log** tab provides the following widgets to visualize the statistical data of the event logs from your devices.

Tip
The **Overview** > **Event Log** page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Widget	Description
Logs Over Time	This widget displays a line chart to visualize the number of log entries over the specified period of time. **Tip** • Click ··· to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time.
Top 5 Service Error Logs	This widget displays the five services that have the largest numbers of error log entries.
Top 5 Service Warning Logs	This widget displays the five services that have the largest numbers of warning log entries.

Monitoring Access Logs

The **Overview** > **Access Log** tab provides the following widgets to visualize the statistical data of the access logs from your devices.

Tip
The **Overview** > **Access Log** page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Section	Description
Logs Over Time	This widget displays a line chart to visualize the number of log entries over the specified period of time. **Tip** • Click ··· to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time.
Currently Online	This widget lists the current online users and provides the information of their user sessions.
Connection Types	This widget displays a pie chart to visualize the numbers of user sessions for each communication protocol.
Logged in	This widget displays a pie chart to visualize the numbers of successful login attempts using each IP address or user account.
Failed to log in	This widget displays a pie chart to visualize the numbers of failed login attempts using each IP address or user account.

Monitoring Online Users

From the **Local Device** > **Online Users** screen, you can find a list of online users and related information such as login date and time, username, source IP address, computer name, connection type, accessed resources, and total connection time.

You can perform the following tasks:

Tasks	Steps
Remove a connection	**1.** Locate a user from the list. **2.** Right-click the user. **3.** Select **Disconnect**. A confirmation message appears. **4.** Click **Yes**.
Control the visible columns	**1.** Click +. **2.** Select the item category to display.

Local Device Logs

The **Local Device** screens allow you to monitor event logs, access logs, and online user status on one local device. You can also configure log filters, log settings, and remove event indicators.

Managing Local Logs

You can monitor and manage event logs and access logs on the local device.

Tip
QuLog Center can store up to 5,000,000 access or event log entries but can only query and process up to 100,000 log entries at a time. By default, the most recent logs are displayed first. You can perform a search to locate earlier logs.

1. Go to **Local Device**.
2. Click **Event Log** or **Access Log.**
3. On the selected system log screen, you can perform the following tasks:

Task	Steps
Select a group mode	**a.** Click . **b.** Select one of the following grouping modes. • **No grouping**: Displays and lists all log entries. • **By date**: Groups log entries by date. • **By user**: Groups log entries by users. • **By Source IP**: Groups log entries by source IP address. Select one of the group modes for event logs. • **By app**: Groups log entries by app name. • **By content**: Groups log entries by log content.
Select a display style	**a.** Click . **b.** Select a display style.
Export logs	**a.** Click . The **Export Logs** window appears. **b.** Select an export file format. **Note** QuLog Center supports CSV and HTML log file formats. **c.** Optional: Compress the export file and specify a password. **d.** Click **Export**. The export file is downloaded by your browser.
Perform a search	**a.** Specify keywords in the search field. **Tip** For advanced search options, click . **b.** Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Searching and Creating Filter Tabs for Logs.
Filter by severity	The severity buttons allow you to filter the currently displayed logs by their severity level. **a.** Click one more severity filter buttons. Only the logs that match the present search conditions and severity filters are displayed.
Select display items	**a.** Click . **b.** Select the item category to display.

Task	Steps
Select all log entries	**a.** Select one or more log entries. **b.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **c.** Click **Select all**.
Invert selection	**a.** Select one or more log entries. **b.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **c.** Click **Invert selection**.
Copy one or more log entries	**a.** Select one or more log entries. **b.** Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	**a.** Select one or more log entries. **b.** Click . A confirmation message appears. **c.** Click **Yes**.

4. On the **Event Log** screen, you can perform the following tasks:

Task	Steps
Create an event notification rule	You can quickly create an event notification rule using a log entry. This allows you to receive notifications for events similar to the selected log entry. **a.** Locate a log entry. **b.** Click . **c.** Select **Create event notification rule**. Notification Center opens and the **Create event notification rule** windows appears. For details, see Creating an Event Notification Rule.
Create an event flag rule	**a.** Locate a log entry. **b.** Click . **c.** Select **Create Event Flag Rule**. The **Create Event Flag Rule** window appears. **d.** Click **Create**. The event is flagged. Go to **Log Settings** > **Event Indicators** to view all event flags.

Searching and Creating Filter Tabs for Logs

You can create custom filter tabs for local event logs and local access logs. These customized filter tabs can filter logs or user information based on specified keywords or criteria.

1. Open QuLog Center.
2. Go to **Local Device** .
3. Click **Event Log** or **Access Log**.
4. Go to the search bar.
5. Click .
   The **Advanced Search** window appears.
6. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click . **b.** Select a severity level option from the drop-down menu.
Date	**a.** Click . **b.** Select a date option from the drop-down menu.
User	**a.** Click . **b.** Select a condition from the drop-down menu. **c.** Specify the keywords.
Source IP	**a.** Click . **b.** Select a condition from the drop-down menu. **c.** Specify the source IP address.
Client App	**a.** Click . **b.** Select a condition from the drop-down menu. **c.** Specify the client app.
The following filter fields are specific to event logs:	
Service	**a.** Click . **b.** Select a service from the drop-down menu. The **Category** option appears. **Note** The **Category** option does not appear if you select any services or do not specify the service. **c.** Specify the service **Category**.

Fields	Steps
Content	**a.** Click ▾. **b.** Select a condition from the drop-down menu. **c.** Specify the content keywords.
Flag	**a.** Click ▾. **b.** Select a flag option from the drop-down menu.
The following filter fields are specific to access logs:	
Connection Type	**a.** Click ▾. **b.** Select a connection type from the drop-down menu.
Action	**a.** Click ▾. **b.** Select an action option from the drop-down menu.

7. Click **Search**.
   The list of filtered results is displayed.
8. Click **Add as Customized Tab**.
   The **Add as Customized Tab** window appears.
9. Enter a tab name.
10. Click **Apply**.
    The custom filter tab is created and displayed next to the **Main** tab.

Local Log Settings

Log Settings allows you to configure the following types of settings: event logs, access logs, display styles, and event indicators.

Configuring Event Log Settings

You can specify the database size and the log language or delete all the log entries for event logs.

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Event Log Settings** .
3. Specify the following settings:

Settings	Steps
Maximum number of entries	**a.** Click ▾. The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed. The log database size is specified.

Settings	Steps
Log retention time	**a.** Click ▾. The log retention time drop-down menu appears. **b.** Select the log retention time.

4. Optional: Delete all event logs.
   a. Click **Delete All Event Logs**.
   A confirmation message appears.
   b. Click **Yes**.

Warning
You cannot restore deleted logs.

5. Select the log language.
   a. Click ▾.
   The log language drop-down menu appears.
   b. Select a language.
6. Click **Apply**.

Configuring Access Log Settings

You can specify the database size, log retention time, connection type, or delete all access log entries.

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Access Log Settings** .
3. Specify the following settings:

Settings	Steps
Maximum number of entries	**a.** Click ▾. The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed.
Log retention time	**a.** Click ▾. The log retention time drop-down menu appears. **b.** Select the log retention time.
Connection Types	Select the connection types you want to log. **Tip** You can select multiple connection types.

4. Optional: Delete all access logs.
   a. Click **Delete All Access Logs**.
   A confirmation message appears.

b. Click **Yes**.

Warning
You cannot restore deleted logs.

5. Click **Apply**.

Configuring a Display Style

You can customize your log display style to enhance readability or to highlight certain entries.

1. Open QuLog Center.
2. Open **Display Settings** through one of the following methods:

Log type	Steps
Event Log	Go to **Local Device** > **Event Log** > **Display style** .
Access Log	Go to **Local Device** > **Access Log** > **Display style** .

3. Click .
   The display style drop-down menu appears.
4. Click **Settings**.
   The **Display Style Settings** window appears.
5. Perform one or more of the following tasks:

Task	Steps
Add a display style	a. Click **Add Style**. The **Add Style** window appears. b. Specify a name for the style. c. Click **Apply**.
Delete a style	a. Select a display style. b. Click **Delete Style**. A confirmation message appears. c. Click **Yes**.
Add a rule to a display style	a. Select a display style. b. Click **Add Rule**. The **Style Rule** window appears. c. Select a field. d. Select a keyword. e. Select one or more formatting effects. **Tip** You can instantly preview the results of the selected formatting effects. f. Click **Apply**.

Task	Steps
Edit a rule	**a.** Select a display style. **b.** Select a rule from the list. **c.** Click **Edit**. The **Style Rule** window appears. **d.** Select a field. **e.** Specify the condition. **f.** Select one or more formatting effects. **Tip** You can instantly preview the results of selected formatting effects. **g.** Click **Apply**.
Remove a rule	**a.** Select a display style. **b.** Select a rule from the list. **c.** Click **Delete**. A confirmation message appears. **d.** Click **Yes**.
Specify the priority of rules	**a.** Select a display style. **b.** Select a rule from the list. **c.** Beside **Priority**, click ^ or v to change its priority. **Note** The formatting results of rules with a higher priority overwrite those with a lower priority.

Removing Event Indicators

1. Open QuLog Center.
2. Go to **Local Device** > **Log Settings** > **Event Indicators** .
3. Select an event flag rule.

Tip
Click the box in the top left column to select all event flag rules.

4. Click **Remove** or .

The event flag rule is removed.

QuLog Service

QuLog Service allows you to centrally manage logs from multiple remote devices. You can configure a single device as a Log Receiver to manage and monitor all incoming system logs from other devices, or configure the device as a Log Sender that sends all system logs to a remote QuLog Center.

Important
QuLog Service requires the device to have an application volume set up. For details, see Application Volume.

Configuring Log Sender Settings

The Log Sender allows you to send event logs and access logs on the local device to a remote QuLog Center or Syslog Server.

Sending System Logs to a Remote QuLog Center

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Sender** > **Send to QuLog Center** .
3. Enable **Send logs to remote QuLog Center**.
4. Event logs and access logs from the local device are sent to a remote QuLog Center.
5. Add a new destination or edit an existing destination:

Options	User Actions
Add a destination IP address	**a.** Click **Add Destination**. The **Add Destination** window appears. **b.** Specify the following IP address information: • **Hostname/IP Address** **Tip** You can enter the hostname or destination IP address manually or click **Search** to automatically select a device from your local network. • **Port** • **Transfer protocol** • **Log type** • **Format** **Note** You can click **Send a Test Message** to test the connection.

Options	User Actions
Edit a destination IP address	**a.** Select a destination IP address. **b.** Click . The **Edit Destination** window appears. **c.** Edit the IP address information.
Remove a destination IP address	**a.** Select one or multiple destination IP addresses. **b.** Click **Remove** or . A confirmation message window appears. **c.** Click **Yes**. The destination IP address is removed.

6. Click **Apply**.
   Changes to the destination IP address are applied.

Sending System Logs to a Syslog Server

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Sender** > **Send to Syslog Server** .
3. Enable **Send logs to remote syslog server**.
4. Select one of the following actions:

Options	User Actions
Add a destination IP address	**a.** Click **Add Destination**. The **Add Destination** window appears. **b.** Specify the following IP address information: • **Destination IP** **Tip** You can enter the destination IP address manually or click **Search** to automatically select a device from your local network. • **Port** • **Transfer protocol** • **Log type** • **Format** **Note** You can click **Send a Test Message** to test the connection.

Options	User Actions
Edit a destination IP address	**a.** Select a destination IP address. **b.** Click . The **Edit Destination** window appears. **c.** Edit the IP address information.
Remove a destination IP address	**a.** Select one or multiple destination IP addresses. **b.** Click **Remove** or . A confirmation message window appears. **c.** Click **Yes**. The destination IP address is removed.

5. Click **Apply**.
   Changes to the destination IP address are applied.

Configuring Log Receiver Settings

The Log Reciever allows you to configure a local device as the recipient of remote device logs. You can centrally manage and monitor event logs and access logs from remote QNAP devices. Additionally, you can configure customized filters to search for logs efficiently.

Configuring General Settings

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **General Settings** .
3. Select **Receive logs from a remote QuLog Center**.
4. Select transfer protocols and then specify the port number.

Note
QuLog Center supports TCP and UDP protocols.

5. Optional: Click **Enable Transport Layer Security (TLS)**.
6. Select **Event Log** or **Access Log**.
7. Specify the following settings:

Settings	Steps
Maximum number of entries	**a.** Click . The maximum number of entries option drop-down menu appears. **b.** Select the maximum number of entries allowed. The log database size is specified.
Log retention time	**a.** Click . The log retention time drop-down menu appears. **b.** Select the log retention time.

Settings	Steps
Delete all event logs	**a.** Click **Delete All Event Logs**. A confirmation window appears. **Warning** You cannot restore deleted logs. **b.** Click **Yes**.

8. Click **Apply**.

Configuring Log Filters

You can specify log filter conditions for system logs received from multiple sender devices on the Log Receiver to easily locate specific types of logs and monitor large volumes of logs.

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Filter Criteria** .
3. Click **Event Log** or click **Access Log**.
4. Select one of the actions to perform:

Tasks	Steps
Add a filter criteria	**a.** Click **Add Filter Criteria**. The filter criteria window appears. **b.** Specify the following information: • Severity level • User • Source IP • Hostname Specify the following information for event logs: • Service • Category • Content Specify the following information for access logs: • Connection type • Accessed resources • Action
Edit a log filter	**a.** Click . The **Filter Criteria** window appears. **b.** Edit the log filter fields.

Tasks	Steps
Delete a log filter	**a.** Select a filter criteria. **b.** Click . A confirmation window appears. **c.** Click **Yes**.
Import a custom filter criterion	**a.** Click **Add Filter Criteria**. **b.** Go to **Import custom filter criteria from the selected tab**. **c.** Click . The custom filter criteria drop-down menu appears. **d.** Select the custom filter tab from the drop-down menu. The selected custom filter criteria are applied to the log. **Note** For details on how to create a custom filter tab, see Searching and Creating Filter Tabs for Remote Logs from Sender Devices.

5. Click **Apply**.
   All changes are applied.

Configuring Notification Rule Settings

You can configure notification rules in Notification Center. You can also create filters for sending local access logs, QuLog Service event logs, and QuLog Service access logs. QuLog Center can send notifications to recipients when the **Log Receiver** receives event logs or access logs from the **Log Sender**.

1. Open QuLog Center.
2. Go to **QuLog Service** > **Log Receiver** > **Notification Settings** .
3. You can perform any of the following actions:

Setting	Steps
Create a notification rule	**a.** Click **Configure Notification Rule**. Notification Center opens. Follow the instructions on the **Create event notification rule** wizard to add an event notification rule for QuLog Center. For details, see Creating an Event Notification Rule. **Important** You must select the **Transfer status** option in **System Notification Rules** when creating QuLog Center notification rules for receiving local device logs, QuLog Service event logs, and QuLog Service access logs. To enable the **Transfer status** option, go to **Notification Center** > **System Notification Rules** > **QuLog Center** > **Transfer status** .
Edit a notification rule	Click .

Setting	Steps
Enable or disable a notification rule	Click toggle.
Delete a notification rule	**a.** Click . A confirmation message window appears. **b.** Click **Yes**. The notification rule is deleted.
View notification history	Click **View notification history**. Notification Center opens and displays the QuLog Center notification history page.

Viewing and Managing Remote Logs

You can view and manage remote logs under the Sender Devices section in QuLog Center. This section lists all remote devices that send their logs to the QuLog Center on the local device. You can monitor logs from all sender devices or from individual sender devices. QuLog Center can manage up to 500 sender devices on a log receiver.

Managing Remote Logs

You can monitor and manage event logs and access logs from remote devices on a Log Receiver. You can also view logs from each sender device.

Tip
QuLog Center can store up to 5,000,000 access or event log entries but can only query and process up to 100,000 log entries at a time. By default, the most recent logs are displayed first. You can perform a search to locate earlier logs.

1. Go to **QuLog Service** > **Sender Devices** .
2. Select **All Devices** or a specific device.
3. Click **Event Log** or **Access Log.**
4. On the selected system log screen, you can perform the following tasks:

Task	Steps
Select a group mode	**a.** Click . **b.** Select one of the following grouping modes. • **No grouping**: Displays and lists all log entries. • **By date**: Groups log entries by date. • **By user**: Groups log entries by users. • **By Source IP**: Groups log entries by source IP address. • **By host name**: Groups log entries by host names. Select one of the group modes for event logs. • **By app**: Groups log entries by app name. • **By content**: Groups log entries by log content.

Task	Steps
Select a display style	**a.** Click . **b.** Select a display style.
Export logs	**a.** Click . The **Export Logs** window appears. **b.** Select an export file format. **Note** QuLog Center supports CSV and HTML log file formats. **c.** Optional: Compress the export file and specify a password. **d.** Click **Export**.
Perform a search	**a.** Specify keywords in the search field. **Tip** For advanced search options, click . **b.** Optional: Click **Add as Customized Tab** and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Searching and Creating Filter Tabs for Logs.
Filter by severity	The severity buttons allow you to filter the currently displayed logs by their severity level. **a.** Click one more severity filter buttons. Only the logs that match the present search conditions and severity filters are displayed.
Select display items	**a.** Click . **b.** Select the items to display.
Select all log entries	**a.** Select one or more log entries. **b.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **c.** Click **Select all**.
Invert Selection	**a.** Select one or more log entries. **b.** Click **Select multiple entries**. The select multiple entries drop-down menu appears. **c.** Click **Invert selection**.
Copy one or more log entries	**a.** Select one or more log entries. **b.** Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.

Task	Steps
Delete one or more log entries	**a.** Select one or more log entries. **b.** Click . A confirmation message appears. **c.** Click **Yes**.

5. On the **Event Log** screen, you can perform the following tasks:

Task	Steps
Create an event flag rule	You can quickly create an event flag rule using a log entry. **a.** Locate a log entry. **b.** Click . **c.** Select **Create event flag rule**. The **Create Event Flag Rule** window appears. **d.** Click **Create**. The event is flagged. Go to **Log Settings** > **Event Indicators** to view all event flags.

Searching and Creating Filter Tabs for Remote Logs from Sender Devices

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices** .
3. Select a sender device.
4. Click **Event Log** or click **Access Log**.
5. Go to the search bar.
6. Click .
7. Specify the following filter fields:

Fields	Steps
Severity Level	**a.** Click . The severity level drop-down menu appears. **b.** Select a severity level option.
Date	**a.** Click . The date drop-down menu appears. **b.** Select a date option.

Fields	Steps
User	**a.** Click ▾. The user condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Source IP	**a.** Click ▾. The source IP address condition option appears. **b.** Select a condition. **c.** Specify the source IP address.
Host name	**a.** Click ▾. The source host name condition option appears. **b.** Select a condition. **c.** Specify the host name.
The following filter fields are specific to event logs:	
Service	**a.** Click ▾. The service drop-down menu appears. **b.** Select a service. The **Category** option appears. **Note** The **Category** option does not appear if you select any services or do not specify the service. **c.** Specify the service **Category**.
Content	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the content keywords.
Flag	**a.** Click ▾. The flag drop-down menu appears. **b.** Select a flag option.
The following filter fields are specific to access logs:	
Computer Name	**a.** Click ▾. The computer name condition option appears. **b.** Select a condition. **c.** Specify the computer name.

Fields	Steps
Accessed Resources	**a.** Click ▾. The content condition option appears. **b.** Select a condition. **c.** Specify the keywords.
Connection Type	**a.** Click ▾. The connection type option appears. **b.** Select a connection type.
Action	**a.** Click ▾. The action drop-down menu appears. **b.** Select an action option.

8. Optional: Click **Reset** to clear all search filters.
   Respecify search filters as many times as required.
9. Click **Search**.
   The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
    The **Add as Customized Tab** window appears.
11. Enter a tab name.
12. Click **Apply**.
    - The custom filter tab is created.
    - The custom filter tab is displayed next to the **Main** tab.

Logging in to a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices** .
3. Select a device.
4. Click **Settings**.
5. Specify the following:
   - **Host IP address**
   - **Port**
   - **Username**
   - **Password**
6. Optional: Select **Secure login (HTTPS)**.
7. Click **Sign in**.
   - You are logged into the sender device.

- All destination IP addresses of the sender device are listed.
- You can configure the destination for sender device logs.
  For details, see the following topics:
  - Sending System Logs to a Remote QuLog Center
  - Sending System Logs to a Syslog Server

Configuring Event Indicators on the Sender Device

The event severity indicators on the device list are displayed according to the event severity level (information, warning, and error) that occurs over a specified period. Only the highest severity level icon is displayed when multiple events occur.

1. Open QuLog Center.
2. Go to **QuLog Service** > **Sender Devices** .
3. Select a device.
4. Got to the **Event Indicators** tab.
5. Click .
   The event period drop-down menu appears.
6. Select the event period.
   Events that meet the specified criteria are listed in the Event Flag Rules table below.

Tip
You can remove event flag rules from the list.

17. Notification Center

Notification Center consolidates all device notifications to help you monitor the status of your device and its applications and address potential issues more closely and promptly. You can send notifications to recipients through different channels including emails, SMS, instant messaging, and other push services. To receive system event notifications, Notification Center also lets you create custom notification rules and criteria, ensuring that you receive event notifications that are most relevant to your needs.

Service Account and Device Pairing

Service Account and Device Pairing allows you to configure the simple mail transfer protocol (SMTP) and short message service center (SMSC) settings so you can receive notifications through email and SMS. You can also pair your instant messaging accounts and devices with your QNAP device to receive notifications through instant messaging or push services.

Email Notifications

The **Email** screen allows you to add and view email notification recipients, and also configure the SMTP service settings.

Button	Task	User Action
	Send a test message to the specified recipient	1. Click  . 2. Specify an email address. 3. Click **Send**.
	Edit configurations of an existing email server	1. Click  . The **Edit SMTP Service Account window** appears. 2. Edit the email account settings. 3. Optional: Click **Re-authorization**. The configured email account is authorized again. 4. Optional: Click **Authenticate with Browser Station**. For details, see Pairing Notification Center with a Web Browser. 5. Optional: Click **Set as the default SMTP service account**. 6. Click **Confirm**.
	Delete an email server	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Configuring an Email Notification

Tip

QNAP recommends you log into your third party email service account before configuring email notifications in Notification Center to skip account verification steps.

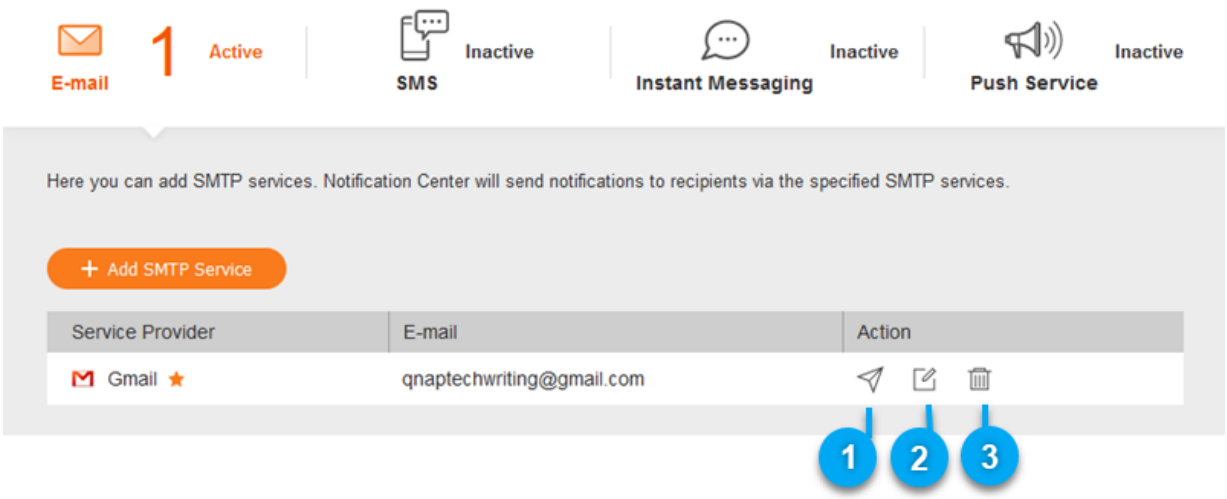
1. Go to **Service Account and Device Pairing** > **E-mail** .
2. Click **Add SMTP Service**.
   The **Add SMTP Service** window appears.
3. Select an email account.
4. Configure the following.

Service Providers	User Actions
Gmail or Outlook	**a.** Click **Add account**. The email account window appears. **b.** Specify the email address that will act as the sender for device notifications. A confirmation message appears. **c.** Click **Allow**.
Yahoo	**Important** You must configure settings in Yahoo Mail before specifying your account information in Notification Center. You must perform the following steps in Yahoo Mail: **a.** Log in to your Yahoo Mail account. **b.** Go to **Help** > **Account Info** > **Account Security** . **c.** Enable **Allow apps that use less secure sign in**. Return to **Notification Center** and specify a valid Yahoo mail address and password.
Custom	**a.** Specify the domain name or the IP address of your SMTP service such as `smtp.gmail.com`. **b.** Specify the port number for the SMTP server. If you specified an SMTP port when you configured the port forwarding settings, use this port number. **c.** Specify the email address that will act as the sender for device notifications. **d.** Specify a username that contains a maximum of 128 ASCII characters. **e.** Specify a password that contains a maximum of 128 ASCII characters. **f.** Select one of the following secure connection options. • **SSL**: Use SSL to secure the connection. • **TLS**: Use TLS to secure the connection. • **None**: Do not use a secure connection. QNAP recommends enabling a secure connection if the SMTP server supports it.
Others	Specify a valid email address and its account password.

Tip
To configure multiple email servers, click **Add SMTP Service**, and then perform the previous steps.

5. Optional: Select **Set as default SMTP service account**.
6. Optional: Click .
   The SMTP server sends a test email.
7. Click **Create**.
   Notification Center adds the SMTP service to the list.

Managing Email Notifications



No.	Tasks	User Actions
1	Send a test message to a specified recipient.	1. Click . The **Send test message** window appears. 2. Specify an email address. 3. Click **Send**.
2	Edit the configurations of an existing email server.	1. Click . The **Edit SMTP Service Account** window appears. 2. Edit the settings. 3. Click **Confirm**.
3	Remove an email server.	1. Click . A confirmation message appears. 2. Click **Confirm**.

SMS Notifications

The **SMS** screen allows you to view and configure the short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Vonage (Nexmo), and Twilio.

Button	Task	User Action
	Send a test message to a specified recipient	1. Click  . The **Send test message** window appears. 2. Specify a country code and phone number. 3. Click **Send**.
	Edit configurations of an existing SMS server	1. Click  . The **Edit SMSC Service Account window** appears. 2. Edit the settings. 3. Click **Confirm**.
	Delete an email server	1. Click  . A confirmation message appears. 2. Click **Confirm**.

Configuring an SMS Notification

1. Go to **Service Account and Device Pairing** > **SMS** .
2. Click **Add SMSC Service**.
   The **Add SMSC Service** window appears.
3. Select a service provider.
4. Specify an alias.
5. Specify the following information.

SMS Service Provider	Information
Clickatell - Communicator/Central	Clickatell username, password, and API ID
Clickatell - SMS Platform	Clickatell API key
Vonage (Nexmo)	Vonage API key and secret question, and a sender name The sender name can contain a maximum of 32 characters.
Twilio	Your Twilio account SID, access token, and the Twilio-provided phone number linked to your account

SMS Service Provider	Information

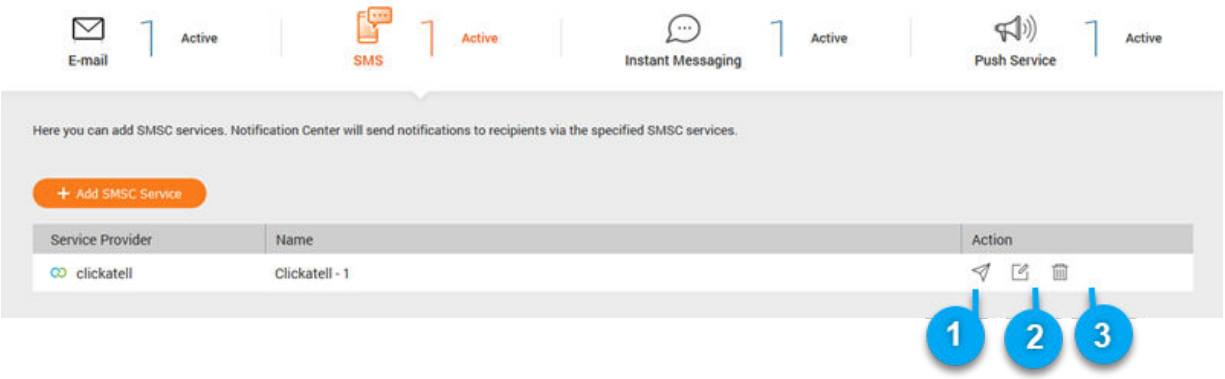
Custom	• URL template text formatted according to the format specified by your SMS service provider.
	Use the following replaceable URL template parameters.
	  • `@@UserName@@`: Specify the username for this connection.
	  • `@@Password@@`: Specify the password for this connection.
	  • `@@PhoneNumber@@`: Specify the phone number where the SMS messages are sent. This parameter is required.
	  • `@@Text@@`: Specify the text content of the SMS message. This parameter is required.
	Important
	You cannot receive SMS messages if the template text does not match the format used by your SMS service provider.
	• The name of the service provider. The name can contain a maximum of 32 ASCII characters.
	• A password. The password can contain a maximum of 32 ASCII characters.

Tip
To configure multiple SMS servers, click **Add SMSC Service**, and then perform the previous steps.

6. Click .
The SMS server sends a test message.

7. Click **Create**.
Notification Center adds the SMS service to the list.

Managing SMS Notifications



No.	Tasks	User Actions
1	Send a test message to a specified recipient.	1. Click . The **Send test message** window appears. 2. Specify a country code and phone number. 3. Click **Send**.
2	Edit the configurations of an existing SMS server.	1. Click . The **Edit SMSC Service Account** window appears. 2. Edit the settings. 3. Click **Confirm**.
3	Remove an SMS server.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Instant Messaging Notifications

The **Instant Messaging** screen allows you to pair Notification Center with instant messaging accounts such as Skype. Notification Center sends notifications to the specified recipients through QBot, the QNAP instant messaging bot account.

Button	Task	User Action
	Send a test message	Click .
	Unpair from and remove the instant messaging account	1. Click . A confirmation message appears. 2. Click **Confirm**.

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure that:

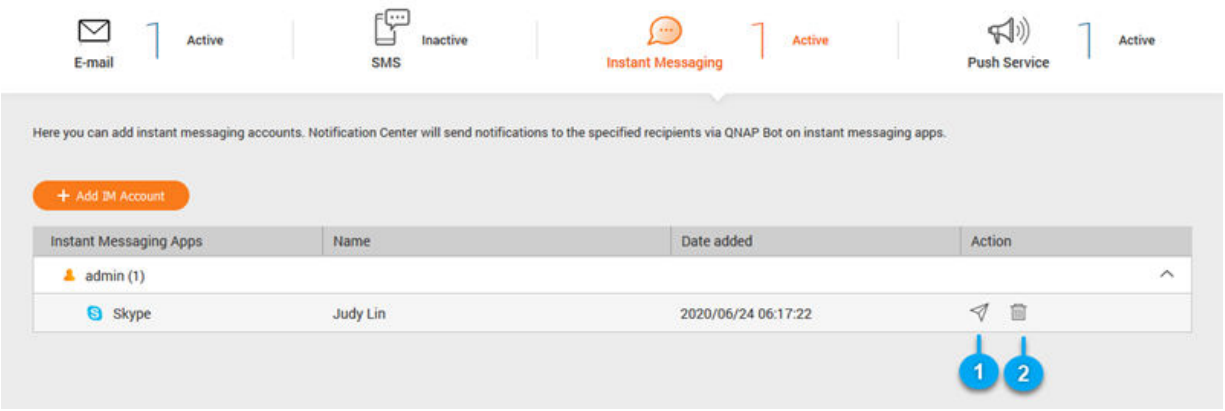
- Your device is registered to an active myQNAPcloud account.
- You have an active Skype account.
- Skype is installed on your device.

1. Go to **Service Account and Device Pairing** > **Instant Messaging** .
2. Click **Add IM Account**.
   The **Notification IM Wizard** appears.
3. Select Skype.
   The **Add Bot to Contacts** window appears.
4. Log in to the Skype account you want to pair.

Skype adds QNAP Bot as a contact.

5. Close the **Add Bot to Contacts** window.
6. Click **Next**.
   A verification code appears.
7. On Skype, enter the verification code.
   Notification Center verifies and pairs with the Skype account.
8. Click **Finish**.
   Notification Center adds the Skype account to the list.

Managing Instant Messaging Notifications



No.	Tasks	User Actions
1	Send a test message.	Click .
2	Unpair and remove the instant messaging account.	1. Click . A confirmation message appears. 2. Click **Confirm**.

Push Notifications

The **Push Service** screen allows you to configure push services for web browsers and mobile devices. Notification Center supports pairing the application with multiple third-party push notification services.

Pairing Notification Center with a Mobile Device

Before pairing, ensure that:

- Your device is registered to an active myQNAPcloud account.
- Qmanager iOS 1.8.0 or Qmanager Android 2.1.0 (or later versions) is installed on your mobile device.
- Your device is added to Qmanager.

1. Open Qmanager on the mobile device.
2. Perform one of the following.

Pairing Option	User Action
Automatic pairing	**a.** From the device list, click the device you want to pair. A confirmation message appears. **b.** Click **Confirm**.
Manual pairing	**a.** Identify your device from the device list, and then click  . The device settings screen appears. **b.** Select **Push notifications**. **c.** Click **Save**. A confirmation message appears. **d.** Click **Confirm**.

Notification Center pairs with the mobile device.

3. In Notification Center, go to **Service Account and Device Pairing** > **Push Service** .
4. Verify that the mobile device appears in the list of paired devices.

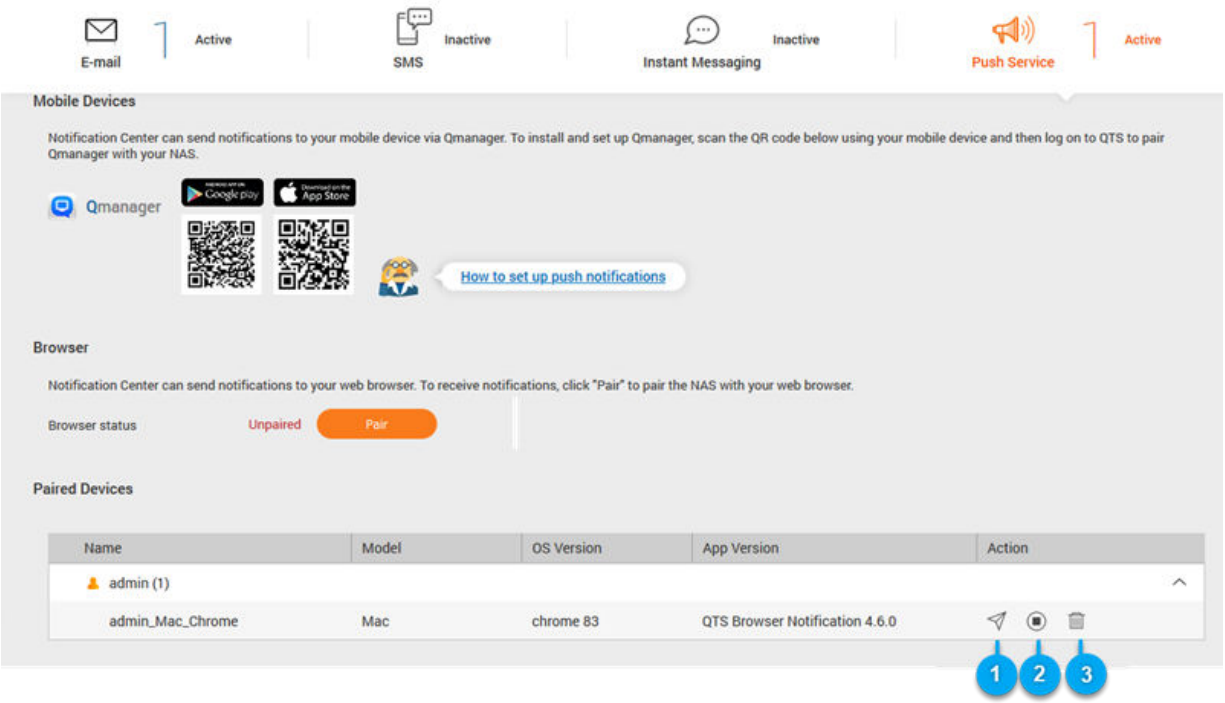
Pairing Notification Center with a Web Browser

Before pairing, ensure that:

- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers:
  - Chrome (version 42 or later)
  - Firefox (version 50 or later)
  - Safari (version 13 or later)
  - Edge (version 96 or later)

1. Go to **Service Account and Device Pairing** > **Push Service** .
2. Under **Browser**, click **Pair**.
   Notification Center pairs with your current browser.
   The browser appears in the list of paired devices.
3. Change your browser name.
   a. Beside your browser name, click  .
   b. Specify a browser name.
   The field accepts up to 127 ASCII characters.
   c. Press **ENTER**.
   Notification Center saves your browser name.

Managing Push Notifications



No.	Tasks	User Actions
1	Send a test message.	Click .
2	Start sending push notifications to the device or browser.	Click .
	Stop sending push notifications to the device or browser.	Click .
3	Unpair and remove the device or browser.	1. Click . A confirmation message appears. 2. Click **Confirm**.

System Notification Rules

You can create and manage event notification rules in the **Event Notifications** page to receive event notifications promptly.

You can also configure alert notifications to specified recipients in the **Alert Notifications** page by setting the alert severity levels.

Creating an Event Notification Rule

1. Go to **System Notification Rules**.
2. Click **Create Rule**.
   The **Create event notification rule** window appears.

3. Specify a rule name.
4. Select the events you want recipients to be notified of.

Tip
To select all events, select **Select all**.
To display only the events for a specific application or service, select the item from the **Displayed Items** drop-down menu.

5. Click **Next**.
6. Select one or more severity levels.

Severity Level	Description
Information	Information messages inform users of changes in the device settings or its applications.
Warning	Warning messages inform users of events when device resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable device features.

7. Specify a keyword filter.

Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click +, and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click +, and then specify one or more keywords.

Important
The event notification filter only accepts keywords that are in English or in any of the languages specified on the **System Notification Rules** screen.

8. Specify a time range when you want to receive notifications.
9. Click **Next**.
10. Select a delivery method.
11. Configure the sender information.

Method	User Action
Email	**a.** Select an SMTP server. **Tip** To add an SMTP server, see Configuring an Email Notification. **b.** Select an e-mail account. **c.** Enter the email address. **d.** Click **Add account**. **e.** Optional: Select **Set as the default SMTP service account**. The configured email service will become the default SMTP service account. **f.** Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive. **g.** Optional: Select **Send email as plain text**.
SMS	Select an SMSC server. **Note** To add an SMSC server, see Configuring an SMS Notification.
Instant Messaging or Push Service	Notification Center automatically assigns QBot.

12. Configure the recipient information.

Method	User Action
Email	**a.** Click **Select User**. The **Select User** window appears. **b.** Select one or more users. **c.** Click **Finish**. The **Select User** window closes. **Tip** • To add a recipient, click **Add**, and then specify their email address. • To delete a recipient, click .

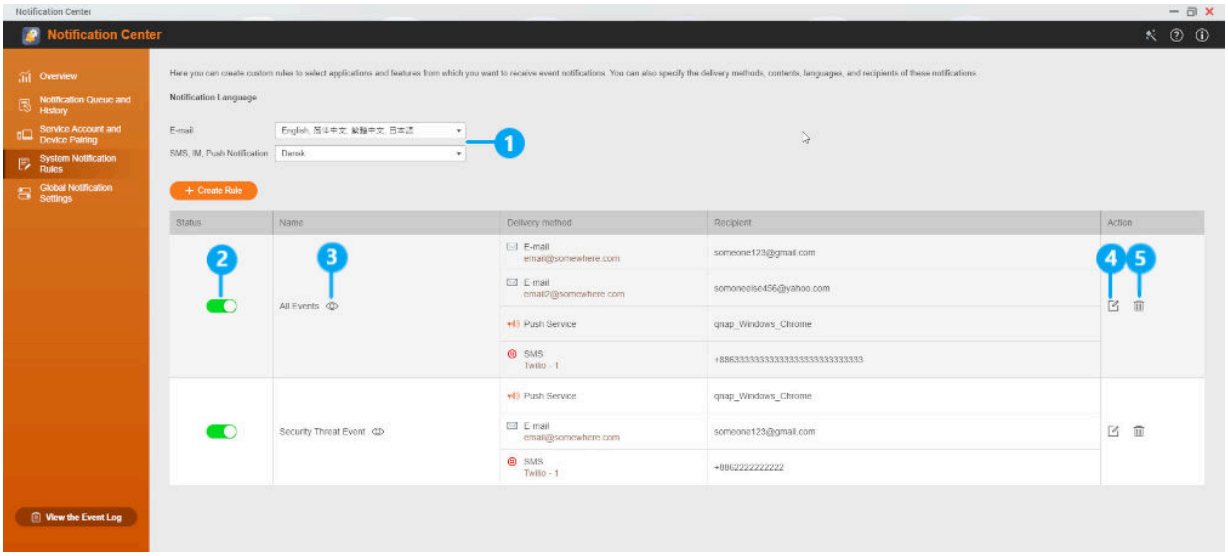
Method	User Action
SMS	**a.** Click **Select User**. The **Select User** window appears. **b.** Select one or more users. **c.** Click **Finish**. The **Select User** window closes. **d.** Select a country code for each recipient. **Tip** • To add a recipient, click **Add**, and then specify their cell phone number. • To delete a recipient, click .
Instant Messaging	Select one or more recipients. **Tip** To add instant messaging notification recipients, see the following topic: Pairing Notification Center with Skype
Push Service	Select one or more recipients. **Tip** To add push notification recipients, see the following topics: • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

13. Optional: Click to send a test message.
14. Optional: Click **Add Pair** to create a new pair.
15. Click **Next**.
16. Verify the rule settings.
17. Click **Finish**.
    Notification Center displays the new rule on the **System Notification Rules** screen.

Managing Event Notification Rules

The **System Notification Rules** screen allows you to create and customize rules to send notifications to target recipients. To send notifications, you must first create and enable rules that determine which application event triggers the outbound notification. You can customize the message type, delivery method, keywords, and time range to further define notification types or narrow the scope.

Notification Center supports sending event notifications in multiple languages and provides four delivery methods including emails, SMS, instant messaging, and push services.



Label	Tasks	User Actions
1	Specify a notification language	**1.** Select one or more languages for email notifications. **Tip** Email notifications contain the notification message repeated in all selected languages. **2.** Select a language for SMS, IM, and push notifications.
2	Enable or disable the rule	Click .
3	Preview rule settings	**1.** Click . The **Event Notifications** window appears. **2.** Review the settings, and then click **Close**.
4	Edit the rule	**1.** Click . The **Edit Rule for Event Notifications** window appears. **2.** Edit the settings. **3.** Click **Confirm**.
5	Delete a rule	**1.** Click . A confirmation message appears. **2.** Click **Confirm**.

Notification Management

You can monitor queuing notifications in Notification Center, view the history of delivered notification messages, configure global notification settings, or monitor important event logs.

Managing Notification Queue and History

Notification Center allows you to view notification queues and notification history. You can view pending notification messages that Notification Center will send on the **Queue** screen, or go to the **History** screen to view all delivered notification messages.

Queue

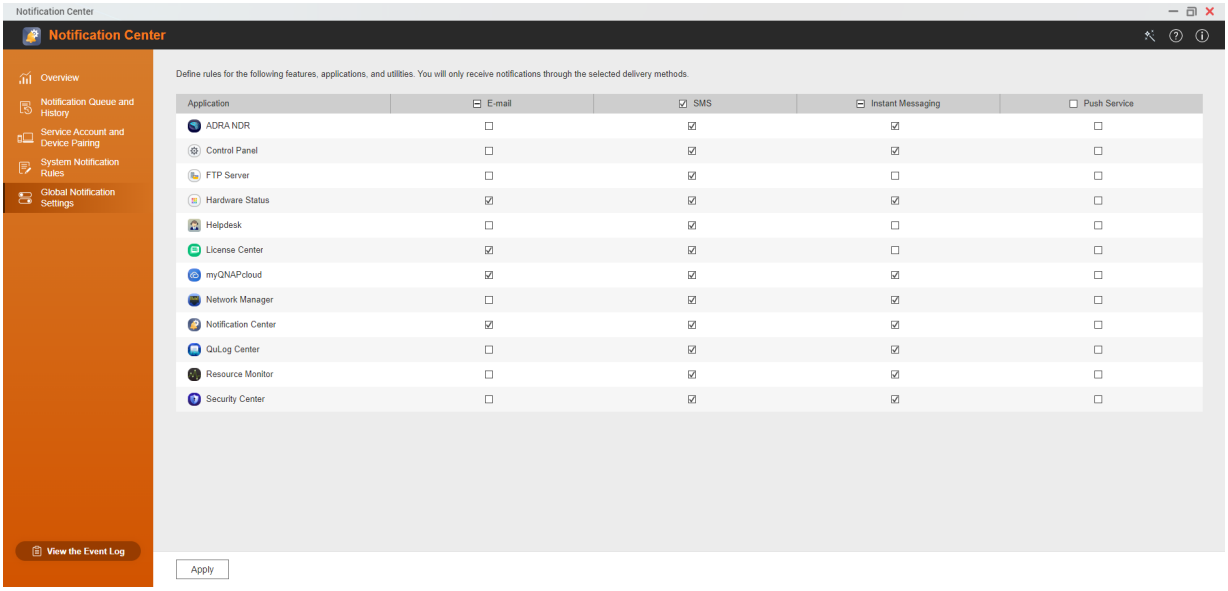
The **Queue** screen displays the messages that Notification Center is going to send. The required transmission time depends on the current status of your device. You can remove messages at any time before they are sent. Removed messages do not appear on the **History** screen.

History

The **History** screen displays the messages that Notification Center has sent. You can view details, resend messages, configure settings, and export the history as a CSV file. You can also specify how long notification records are retained and where they are stored in **Settings**.

Tasks	User Actions
Export the notification message history.	Click **Export**. Notification Center saves the CSV file on your computer.
Resend the notification.	Identify the notification you want to resend, and then click  . This button only appears when Notification Center is unable to send the notification to the recipient.
Configure the history settings.	1. Click **Settings**. The **Settings** window appears. 2. Specify the maximum number of days to retain notification records before deletion. 3. Click **Confirm**. Notification Center saves your settings.

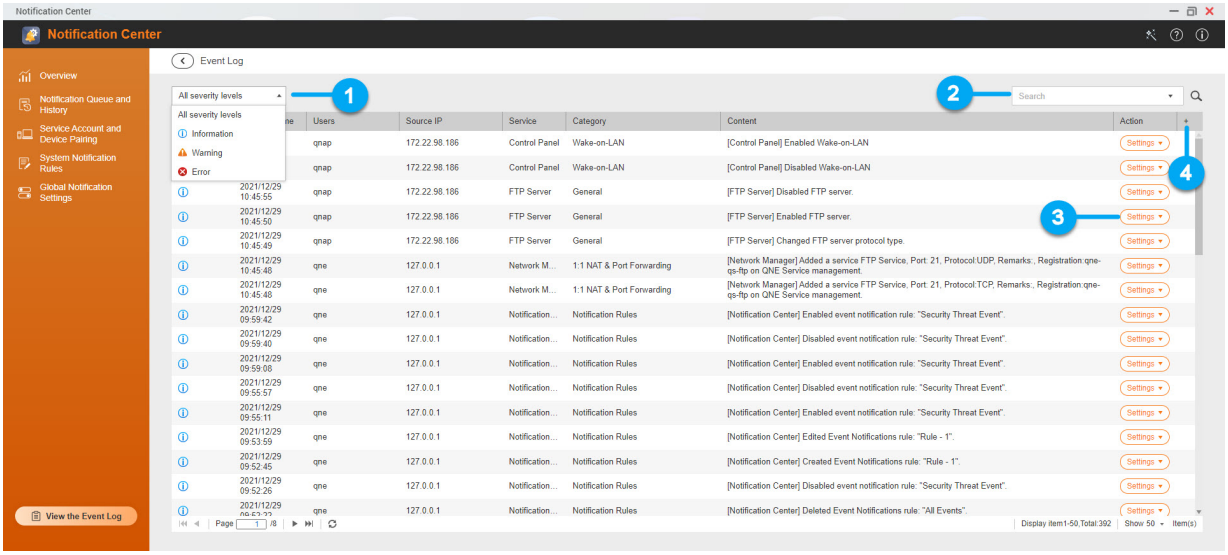
Configuring Global Notification Settings



The **Global Notification Settings** screen allows you to quickly configure notification methods for each device feature or application. Users will only receive notifications through the specified delivery channels.

Viewing Event Logs

Go to **View the Event Log** to view all system events on the device. On this screen, you can sort and filter the logs or create notification rules based on existing logs.



No.	Tasks	User Actions
1	Filter system logs	Select a severity level.

No.	Tasks	User Actions
2	Search logs	You can search logs using simple search or advanced search methods. Simple search: Enter terms into the search box. Event logs whose Content field matches the search terms are displayed. Advanced search: **1.** Click ▼. The **Advanced Search** window appears. **2.** Specify the following: • Keywords • Severity Level • Date • Source IP • Service • Category • Users • Client App **3.** Click **Search**. A list of event logs that meet the search criteria is displayed.
3	Create a notification rule	**1.** Locate an event to create a notification rule for. **2.** Click **Settings**. **3.** Click **Create event notification rule**. The **Create notification rule** window appears. **4.** Select one of the following options. • **Add as a new rule** • **Add to an existing rule** **5.** Click **Confirm**. **Tip** To add or edit notification rules, see Creating an Event Notification Rule.
4	Select display items	**1.** Click +. **2.** Select the items to display.

18. Security Center

Security Center is a utility that centralizes security settings. From Security Center, you can download and replace SSL certificates as well as update the password policy. Additionally, our powerful anti-tampering features can detect and record unauthorized changes to your device and restore modified files to their original state.

Running a Security Checkup

Security Checkup reviews specific settings defined by your Security Policy and provides suggestions for improving the security of your device.

1. Open Security Center.
2. Click **Security Checkup**.
3. Click **Start Security Checkup**.
   The **Security Analytics** page appears.
4. Optional: Click **Yes** to send the scan results to QNAP.

Important
When you first open the Security Checkup screen, you can choose a Security Policy and click **Scan Now**. Security Center starts scanning your device.

5. Optional: Select a new Security Policy.
   a. Click ⚙.
      The **Security Policy** window opens.
   b. Click ▼.
      A menu list appears.
   c. Select a Security Policy.

Tip
To learn more about each security policy, click ℹ.

   d. Click **Apply**.
      A confirmation message appears.
   e. Click **OK**.
      A message appears asking to run a security checkup.
   f. Optional: Click **Yes**.
      Security Center starts scanning your device.
6. Optional: Enable a scan schedule.
   a. Near **Scan schedule**, click ✎.
      The **Scan schedule** window opens.
   b. Select **Enable schedule**.
   c. Select one or more days to run the scan schedule.
   d. Select a time to run the scan schedule.

e. Click **Apply**.

7. Click **Scan**.
   Security Checkup scans your device.

Note

- You can check and automatically apply security suggestions. To see a list of security suggestions, click **Suggested Settings Assistant**. Select at least one suggestion to implement and then click **Apply suggestion**.
- You can check and manually apply security suggestions. To see a list of security suggestions, click **Suggested Settings Assistant** and then **Manually**. Under **At-risk User Settings**, click a statement to open the application to fix this risk.
- To see more details about or ignore a result, click ⋮ and select **Description** or **Ignore result**.

Configuring the Password Policy

1. Open Security Center.
2. Click **Password Policy**.
3. Under **Password Strength**, configure any of the following password criteria.

Criteria	Description
English letters	Passwords must contain at least one letter. Select **At least 1 uppercase and 1 lowercase** to require at least one uppercase and one lowercase letter.
Digits	Passwords must contain at least one number.
Special characters	Passwords must contain at least one special character.
Must not include characters repeated three or more times consecutively	Repeating characters are not allowed. For example, `AAA`.
Must not be the same as the associated username, or the username reversed.	The password must not be the same as the username or the reversed username. For example, username: `user1` and password: `1resu`.
Minimum length	The password length must be greater than or equal to the specified number. Specify a value between 4 and 64 characters.

4. Require users to periodically change their passwords.

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

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

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

Note
Specify a number between 1 and 365.

5. Click **Apply**.

A confirmation message appears when you first apply a password policy change.

6. Click **Yes**.
   Security Center applies the password policy changes.

Scanning Applications for Unauthorized File Changes

Scanning allows you to verify application integrity and checks for unauthorized changes to files and data.

1. Open Security Center.
2. Click **Anti-tampering**.

Important
When you open the Anti-tampering screen for the first time, click **Scan** to perform an initial analysis of your device. Security Center checks for tampered applications.

3. Optional: Enable a scan schedule.
   a. Next to **Scan schedule**, click .
      The **Scan schedule** window opens.
   b. Select **Enable schedule**.
   c. Configure the date and time settings.
   d. Click **Apply**.
4. Click **Scan**.
   Security Center scans the installed applications for unauthorized file changes. Results are displayed on the **Scan Results** panel. Previously restored files are displayed on the **Repaired Files** panel.

Tip

- To restore every file with authorized changes to previous version, click **Restore**. You can restore individual files by selecting files before clicking **Restore**.
- To export every result, click **Export**. Results are saved as a .xls file. You cannot export individual results.

SSL Certificate and Private Key

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

Downloading the SSL Certificate and Private Key

1. Open Security Center.
2. Click **Certificate & Private Key**.
3. Click **Download Certificate**.
   A dialog box appears.
4. Select the items to download.

5. Click **OK**.
   QNE downloads the selected files to your computer.

Replacing the SSL Certificate and Private Key

1. Open Security Center.
2. Click **Certificate & Private Key**.
3. Click **Replace Certificate**.
   The **Replace Certificate** window appears.
4. Select an option.

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

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

Option	User Action
Import certificate	**a.** Click **Browse** to upload a valid certificate. **b.** Click **Browse** to upload an intermediate certificate.
Get from Let's Encrypt	**a.** Specify a domain name containing a maximum of 63 ASCII characters, without spaces. **b.** Specify a valid email address. **c.** Optional: Specify an alternative name. **Tip** Use "," to separate multiple aliases. Example: `123.web.com,789.web.com`

Option	User Action
Create self-signed certificate	Configure the following information: • **Private key length** • **Common name** • **Email** • **Country** • **State/Province/Region** • **City** • **Organization** • **Department**

7. Click **Apply**.
   Security Center replaces the SSL Certificate and Private Key.

19. QuFirewall

QuFirewall is a firewall management application which allows you to control and review all incoming connections to your QNAP device.

Installing QuFirewall

Important
QuFirewall is a preinstalled application on QNE. This task explains how to reinstall the application.

1. Log on to QNE.
2. Go to **Application Store**, and then click .
   A search box appears.
3. Enter `QuFirewall`.
   The QuFirewall application appears in the search results.
4. Click **Install**.

QNE installs QuFirewall.

Initializing QuFirewall

This section walks you through the process of configuring QuFirewall. These steps are only required the first time you start QuFirewall.

1. Open QuFirewall.
   The **Get Started** wizard opens.
2. Select a Firewall Profile.

Profile	Description
Basic protection	Allows access only to the regional domains specified during the next step.
Include subnets only	Allows access only to local network sources.
Restricted security	Allows access to frequently used service ports from devices on the local network or regional domains.

3. Click **Next**.
4. Select the region where the device is located.
5. Click **Next**.
6. Optional: Select **Enable firewall**.

Important
You must enable the firewall for QuFirewall to take effect. After initialization, you can also enable or disable the firewall anytime by toggling the **Firewall** switch on the app screen.

7. Click **Finish**.

QuFirewall finishes the initialization process.

Firewall Profiles

A firewall profile allows you to configure a custom set of rules on the types of connections you allow and/or deny. You can create different profiles for different use cases and switch between them when needed.

By default, QuFirewall offers several firewall profiles to get you started.

Important

- You can create up to 10 profiles.
- Each profile can have a maximum of 128 rules.

Creating a Firewall Profile

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Go to **Add Profile** > **Create Profile** .
   The **Create Profile** window opens.
4. Specify a profile name.

Note
The profile name must be between 1 to 32 characters.

- Valid characters: A–Z, a–z, 0–9
- Valid special characters: Space ( ), Hyphen (-), Underscore (_)

5. Add rules.
   a. Click **Add Rule**.
      The **Add Rule** window opens.
   b. Select whether to allow or deny matching connections.
   c. Select the network interface to monitor for connections.
   d. Select a connection source.

Source	User Action
Any	No further action is necessary. **Note** This option applies the rule to all connections.

Source	User Action
IP	Select one of the following: • **Single IP address**: Enter an IP address. • **IP subnet**: Enter an IP address and subnet mask. • **IP range**: Enter an IP range with a lower bound and an upper bound. **Note** This option applies the rule to a single IP address, a specific subnet, or every IP within a specific range.
Region	Click the selection menu to select one or more regions. **Note** • This option applies the rule to IPs originating from one or more specified regions. • You can specify up to 14 regions.

e. Select an IP protocol type.

f. Select a service port.

Note
This field is only available if you select **TCP** or **UDP** in the previous step.

Service Ports	User Action
Any	No further action is necessary. **Note** This option applies the rule to all service ports.
Custom	Enter up to 15 service ports. **Note** • This option applies the rule to the specified ports. • Ports must be between 1 and 65535. • Separate multiple ports with commas (,). • Use hyphens (-) without a space to indicate a port range.
Built-in applications	Click the selection menu to select one or more built-in applications. **Note** This option applies the rule to the specified built-in applications.

g. Click **Apply**.
QuFirewall adds the rule in the **Create Profile** window.

h. Optional: Under **ON**, select the checkbox to activate the rule.

i. Optional: Under **Priority**, click and drag ≡ to change the rule's priority within the list.

Note
Rules higher on the list have priority over rules lower on the list.

6. Click **Create**.
   A confirmation window opens.
7. Click **Yes**.

QuFirewall creates the profile.

Managing a Firewall Profile

This section provides steps for editing, deleting, duplicating, importing, and exporting firewall profiles.

Editing a Firewall Profile

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Identify an existing profile.
4. Under **Action**, click .
   The **Edit Profile** window opens.
5. Optional: Edit the profile name.
6. Optional: Add, edit, and/or delete rules.

Note
For details on adding or editing a rule, see Adding a Rule to a Firewall Profile.

7. Click **Apply**.
   A confirmation window opens.
8. Click **Yes**.

QuFirewall saves the profile.

Deleting a Firewall Profile

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Identify an existing profile.
4. Under **Action**, click .
5. Click **Delete**.
   A confirmation window opens.
6. Click **Delete**.
   QuFirewall deletes the profile.

QuFirewall deletes the profile.

Duplicating a Firewall Profile

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Identify an existing profile.
4. Under **Action**, click ⋮.
5. Click **Duplicate**.
   The **Duplicate Profile** window opens.
6. Optional: Edit the profile name.
7. Optional: Add, edit, and/or delete rules.

> **Note**
> For details on adding or editing a rule, see Adding a Rule to a Firewall Profile.

8. Click **Apply**.
   A confirmation window opens.
9. Click **Yes**.

QuFirewall duplicates the profile.

Importing a Firewall Profile

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Go to **Add Profile** > **Import Profile** .
   A file explorer window opens.
4. Locate an existing firewall profile on your local device.
5. Click **Open**.
   The **Import Profile** window opens.
6. Optional: Edit the profile name.
7. Optional: Add, edit, and/or delete rules.

> **Note**
> For details on adding or editing a rule, see Adding a Rule to a Firewall Profile.

8. Click **Apply**.
   A confirmation window opens.
9. Click **Yes**.

QuFirewall imports the profile.

Exporting a Firewall Profile

1. Open QuFirewall.

2. Click **Firewall Profiles**.
3. Identify an existing profile.
4. Under **Action**, click ⋮.
5. Click **Export**.

QuFirewall prepares the file for download.

Adding a Rule to a Firewall Profile

You can add rules that allow or deny connections based on specific criteria, including the network interface, connection source, and IP protocol.

1. Open QuFirewall.
2. Click **Firewall Profiles**.
3. Identify an existing profile.
4. Under **Action**, click .
   The **Edit Profile** window appears.
5. Click **Add Rule**.

Tip

You can edit an existing rule instead. Identify an existing rule and click under **Action**. The remaining steps are identical for editing a rule.

The **Add Rule** window opens.

6. Select whether to allow or deny matching connections.
7. Select the network interface to monitor for connections.
8. Select a connection source.

Source	User Action
Any	No further action is necessary. **Note** This option applies the rule to all connections.
IP	Select one of the following: • **Single IP address**: Enter an IP address. • **IP subnet**: Enter an IP address and subnet mask. • **IP range**: Enter an IP range with a lower bound and an upper bound. **Note** This option applies the rule to a single IP address, a specific subnet, or every IP within a specific range.

Source	User Action
Region	Click the selection menu to select one or more regions. **Note** • This option applies the rule to IPs originating from one or more specified regions. • You can specify up to 14 regions.

9. Select an IP protocol type.
10. Select a service port.

Note
This field is only available if you select **TCP** or **UDP** in the previous step.

Service Ports	User Action
Any	No further action is necessary. **Note** This option applies the rule to all service ports.
Custom	Enter up to 15 service ports. **Note** • This option applies the rule to the specified ports. • Ports must be between 1 and 65535. • Separate multiple ports with commas (,). • Use hyphens (-) without a space to indicate a port range.
Built-in applications	Click the selection menu to select one or more built-in applications. **Note** This option applies the rule to the specified built-in applications.

11. Click **Apply**.
    QuFirewall saves the rule in the **Edit Profile** window.
12. Optional: Under **ON**, select the checkbox to activate the rule.
13. Optional: Under **Priority**, click and drag ≡ to change the rule's priority within the list.

Note
Rules higher on the list have priority over rules lower on the list.

Configuring GeoIP Update Settings

The GeoIP database identifies the geographic location of a connecting device.

1. Open QuFirewall.

2. Click ⋮, and then click **Settings**.
   The **Settings** window opens.
3. Go to **GeoIP Update**.
4. Select when to update the GeoIP database.

Option	Description
Do not check for GeoIP database update automatically	QuFirewall does not automatically check for GeoIP database updates.
Remind me when checking a new GeoIP database	QuFirewall sends a notification when opening the application if an update to the GeoIP database is available.
Automatically update the GeoIP database	QuFirewall automatically updates the GeoIP database when an update is available.

Tip
Click **Check for Updates** to immediately update the GeoIP database if an update is available.

5. Click **Apply**.

QuFirewall saves the settings.

Firewall and Capture Events

QuFirewall maintains a record of denied connection attempts on the **Firewall Events** screen.

You can instruct QuFirewall to capture more in-depth information on these denied connection attempts, also known as denied packets, on the **Capture Events** screen.

Managing Firewall Events

This section provides steps for filtering and exporting firewall events, and configuring firewall event settings.

Filtering Firewall Events

1. Open QuFirewall.
2. Click **Firewall Events**.
3. Click **Filter**.
   The **Filter** window opens.
4. Specify the filter criteria.

Criteria	User Action
Day Period	Specify a date range for the filtered events.
Time Period	Specify a time period for the filtered events.
Interface	Specify the network interface connected to the filtered events.
Port	Specify the service port connected to the filtered events.

Criteria	User Action
Source	Specify the connection source of the filtered event. • **IP**: Specifies an IP address. • **Location**: Specifies a country.

5. Click **Search**.

QuFirewall filters the firewall events.

Exporting Firewall Events

1. Open QuFirewall.
2. Click **Firewall Events**.
3. Click **Export**.
   A confirmation window opens.
4. Click **Save**.

QuFirewall prepares the file for download to your local device.

Configuring Firewall Event Settings

1. Open QuFirewall.
2. Click ⋮, and then click **Settings**.
   The **Settings** window opens.
3. Go to **Firewall Events**.
4. Configure the settings.

Setting	User Action
Storage Limitation	Specify the number of days to store firewall events.
Event Logging Frequency	Specify how often to log the number of event occurrences.
Alert Messages	Specify the alert message threshold number. After crossing this threshold, QuFirewall registers a warning in the system log.

5. Click **Apply**.

QuFirewall saves the settings.

Capturing Denied Packets

1. Open QuFirewall.
2. Click **Capture Events**.
3. Specify a duration.

Note

- The duration must be between 10 seconds and 30 minutes.

- The default duration is 30 minutes.

4. Click **Start Packet Capture**.

Tip
Click **Stop** to stop the capture process early.

QuFirewall begins capturing denied packets.

5. After the specified duration, click **Save**.

QuFirewall prepares the file for download to your local device.

20. Resource Monitor

You can monitor the status of your device in Resource Monitor.

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

Section	Description
Overview	This screen provides a general summary of CPU usage, memory usage, network usage, and ongoing processes on the device.
System Resource	This screen uses line charts to display CPU usage, memory usage, network usage, and graphics card usage (if supported and installed) over time. You can hover the mouse pointer over a line chart to view the hardware usage at a specific point in time. **Tip** You can click **More** (⋮) and then select **Settings** to specify the time interval on the line charts.
Storage Resource	This screen displays static volume usage. **Note** You can click **Refresh** to refresh the screen.
Processes	This screen displays all ongoing background processes and provides information about each process, such as its current status, CPU usage, and memory usage. **Tip** You can enable **Group by Applications** to group related processes together (for example, all the processes related to an application or a system feature). You can also sort information in ascending or descending order, column category, show or hide columns, and choose to **Collapse All** or **Expand All** running processes. **Note** If your device's CPU processor has 4 cores and 8 threads or above, the **Allocate CPU Resources** window automatically appears.

21. Helpdesk

Helpdesk is a built-in application that allows you to quickly find solutions or contact the QNAP support team when you encounter any issues while using QNE and related applications.

Support Services

On the **Overview** screen, you can contact the QNAP support team, browse frequently asked questions and application notes, download QNAP user manuals, find out how to use a QNAP device, search the QNAP knowledge base, and find compatible devices. This screen also displays Helpdesk message logs.

Title	Description
Help Request	Contact the QNAP support team by submitting your issues or questions.
QNAP Online Tutorial & FAQ	Browse frequently asked questions and application notes for QNAP devices and applications.
User Manual	View or download QNAP device user manuals.
QNAP Helpdesk Knowledge Base	Search the QNAP knowledge base for answers from the support team for different issues.
Compatibility List	Find drives and devices that are compatible with QNAP devices.
My Tickets	View the status of your submitted tickets.

Submitting a Ticket

You can submit a Helpdesk ticket to receive support from QNAP. Helpdesk automatically collects and attaches device system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

1. Open **Helpdesk**.
2. Go to **Help Request**.
3. Sign in with your QNAP ID.
4. Specify the ticket details.

Fields	User Actions
Subject	Specify the subject.
Issue Category	Select an issue category, and then select an issue.
Issue Type	Select an issue type.
Operating System	Select an operating system.
Description	Specify a short description for each issue.

5. Upload the attachments.
    a. Optional: Select **I am allowing QNAP Support to access my system logs**.
    b. Upload screenshots or other related files.

Note

- You can upload up to 8 attachments, including system logs.

- Each file must be less than 5 MB.

6. Specify the following information.

Fields	User Actions
Your Email Address	Specify your email address.
Phone number	Specify your phone number.
Customer type	Select a customer type.
Company name	Specify your company name. **Note** This field only appears when you select Business User as the **Customer type**.
Your timezone	Select a timezone.
Apply the changes to my profile in QNAP Account	Click to apply your profile changes in QNAP Account.
First name	Specify your first name.
Last name	Specify your last name.
Your location	Select a location.

7. Optional: Select **Apply the changes to my profile in QNAP Account**.
8. Click **Submit**.

Enabling Remote Support

Remote Support allows the QNAP support team to directly access your device to help you solve any ongoing issues.

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Specify your ticket ID.
4. Specify your email address.
5. Click **Enable Remote Support**.
   The **QNAP Helpdesk Terms of Service** window appears.
6. Accept the terms of service.
   a. Click **I agree to these Terms of Service**.
   b. Click **Agree**.
      The **Enable SSH** window appears.

Note
Enable Remote Support is only required when you enable the feature for the first time.

7. Click **Yes**.
   The **Enable Remote Support** window appears.
8. Click **Confirm**.
   Helpdesk creates a private key and temporary account.

Extending or Disabling Remote Support

Extending Remote Support allows you to extend the remote session by a week so you can perform the remote session at a specific time. QNAP will notify you about extending the remote session for unsolved issues.

Note
Remote Support is disabled when the support team has completed the remote session, or when the private key has expired.

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Extend** to extend Remote Support or **Disable** to disable Remote Support.

Note
Both **Extend** and **Disable** buttons only appear after Remote Support is enabled.

4. Click **Finish**.

Downloading Logs

The Diagnostic Tool provides download log features for checking the device stability. You can export the system kernel records to quickly check for exceptions or errors that have occurred. In addition, you can send the records to QNAP technical support for further investigation.

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool** > **Download Logs** .
3. Click **Download**.
   Helpdesk generates a ZIP file.
4. Download the ZIP file.
5. Optional: Send the file to QNAP through Help Request for further investigation.

Configuring Settings

1. Open **Helpdesk**.
2. Go to **Overview**.
3. Click .
   The **Settings** window appears.
4. Specify the message retention time.
5. Optional: Click **Retain all messages**.
6. Optional: Click **I am allowing QNAP Support to access my system logs**.
7. Optional: Click **Sign In**.
   The **Settings** window appears.
8. Specify your QNAP ID.

9. Specify the password.
10. Click **Sign In**.
11. Click **Apply**.

22. Console Management

Console Management is a text-based tool that helps you perform some basic configuration or maintenance tasks if you cannot access the device normally or if you do not have direct access to the device. You can use the program with an SSH client and command-line interface. Console Management is accessible only after the operating system has finished initialization.

Access

If you are a Windows user, you must download third-party software to log in to Console Management. macOS users can log in to Console Management through **Terminal**.

Accessing Console Management from Windows

1. Download PuTTY from https://www.putty.org and then follow the on-screen instructions to install the software.
2. Open PuTTY, and type the device's IP address underneath **Host Name (or IP address)**.
3. Select **SSH** as the connection type.

Note
This option is selected by default.

4. Click **Open**.
   The **PuTTY Security Alert** window appears.

Note
This window only appears when you first run the application.

5. Click **Yes**.
   A login screen appears.

Accessing Console Management from Mac

1. Open **Terminal**.
2. Enter `ssh USERNAME@DEVICE_IP`.

Note

- Replace `USERNAME` with the account username.
- Replace `DEVICE_IP` with the device's IP address.

Tip
If you encounter an error, enter `ssh-keygen -R DEVICE_IP`. Replace `DEVICE_IP` with the device's IP address.

A login screen appears.

Logging In to Console Management

1. Enter the username.

2. Enter the password.

Note
For security purposes, the password does not show.

Tip
Do not copy and paste the password to the program.

The **Console Management - Main menu** screen appears.

Applications and Licenses

You can perform basic functions on existing applications and activate and deactivate existing licenses.

Managing Existing Applications

1. Log in to Console Management, and then enter `5`.
   The App window and three options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

Tip
To browse your applications, enter `n` or `p` to go to the next or previous page.

Option	User Action
List installed apps	Enter `1`. Console Management displays a list of all installed applications on the operating system.
List enabled apps	Enter `2`. Console Management displays a list of all enabled applications on the operating system.
List disabled apps	Enter `3`. Console Management displays a list of all disabled applications on the operating system.
Return	Enter `r`. Console Management returns to Main menu.

A list of applications appear.

3. Enter the alphanumeric character corresponding with the application you want to perform an action on.
   Five options appear.
4. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Start	Enter `1`. The application starts.
Stop	Enter `2`. The application stops.
Restart	Enter `3`. The application restarts.

Option	User Action
Remove	Enter `4`. The application is removed. **Note** If an application can't be removed, Console Management tells you that this function is currently unavailable.
Return	Enter `r`. Console Management returns to Main menu.

The system performs the specified action and tells you whether the action has succeeded or not.

Activating or Deactivating a License

1. Log in to Console Management, and then enter `4`.
   Two options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Activate a License	**a.** Enter `1`. **b.** Enter a license activation key.
Deactivate a License	**a.** Enter `2`. **b.** Enter a license activation key.
Return	Enter `r`. Console Management returns to Main menu.

The system performs the specified action.

System Logs and Network Settings

If you cannot access your device normally, checking your system logs and network settings through Console Management could help identify the problem.

Sorting and Filtering System Logs

1. Log in to Console Management, and then enter `2`.
   Eleven options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.

Note
System logs are displayed in the following format: record_id, date, time, user, app_id, application, category_id, category, msg_id, message.

Option	User Action
date in ascending order	Enter `1`. Console Management displays all system logs in ascending order according to the date.

Option	User Action
date in descending order (default)	Enter `2`. Console Management displays all system logs in descending order according to the date.
user in ascending order	Enter `3`. Console Management displays all system logs in ascending order according to the username.
user in descending order	Enter `4`. Console Management displays all system logs in descending order according to the username.
IP in ascending order	Enter `5`. Console Management displays all system logs in ascending order according to the IP address.
IP in descending order	Enter `6`. Console Management displays all system logs in descending order according to the IP address.
app name in ascending order	Enter `7`. Console Management displays all system logs in ascending order according to the application name.
app name in descending order	Enter `8`. Console Management displays all system logs in descending order according to the application name.
category in ascending order	Enter `9`. Console Management displays all system logs in ascending order according to the application category.
category in descending order	Enter `10`. Console Management displays all system logs in descending order according to the application category.

The filter screen appears.

3. Optional: Enter a filter query.

Note

- Ensure all filter conditions follow the relevant on-screen format. For example, filtering by an application name should follow this format: `A={myQNAPcloud}`.
- To filter by multiple conditions, use '&' in between filters. For example, filtering by severity level and an application name should follow this format: `T={0}&A={myQNAPcloud}`.

Filter	User Action
Severity level	**a.** Enter one of the following options. • `T={0}` **Note** This filter only includes system logs classified as information. This type of system log is indicated as ⓘ in QuLog Center. • `T={1}` **Note** This filter only includes system logs classified as warnings. This type of system log is indicated as ⚠ in QuLog Center. • `T={2}` **Note** This filter only includes system logs classified as errors. This type of system log is indicated as ⊗ in QuLog Center. Console Management filters all system logs according to the specified severity level.
Keyword	Enter a keyword. Console Management filters all system logs according to the specified keyword.
Username	Type an username. Console Management filters all system logs according to the specified username.
Source IP	Enter a source IP. Console Management filters all system logs according to the specified source IP.
Application name	Enter an application name. Console Management filters all system logs according to the specified application name.
Category name	Enter an application category. Console Management filters all system logs according to the specified category.

A list of system logs appear.

Tip
To browse your applications, enter `n` or `p` to go to the next or previous page.

Showing Network Settings

1. Log in to Console Management, and then enter `1`.

Note
Network settings appear in the following format: adapter, virtual switch, status, IP, MAC address.

The Network settings window appears.

Device Actions

If you cannot access your device, you can restore specific device settings or reinitialize or reboot the device.

Resetting the Device to Factory Default Settings

1. Log in to Console Management, and then enter `3`.
   The **Reset** window and two options appear.
2. Perform one of the following actions.

Option	User Action
Reset network settings and enable 'system-maintainer'	**a.** Enter `1`. **b.** Enter the password. Console Management resets the network settings.
Reboot to reinitialize the device	**a.** Enter `2`. **b.** Enter the password. Console Management erases all data and reinitializes the device.
Return	Enter `r`. Console Management returns to Main menu.

Rebooting the Device to Safe Mode Without a Configured Disk

1. Log in to Console Management, and then enter `6`.
   The **Reboot in Safe mode** window opens.
2. Enter the password you used to log in to Console Management.
   Console Management reboots the device.