QHora-301W

User Guide

Document Version: 3
12/04/2022

Contents

1. Preface

2. Product Overview

3. Installation and Access

4. QuRouter

5. QuRouter Navigation

6. System Configuration

7. Network Settings

10. Glossary

11. Notices

1. Preface

About This Guide

This guide provides information on the QNAP QHora-301W router and step-by-step instructions on installing the hardware. It also provides instructions on basic operations and troubleshooting information.

Audience

This document is intended for consumers and network administrators. This guide assumes that the user has a basic understanding of network, storage, and backup concepts.

Document Conventions

Symbol	Description
💬	Notes provide default configuration settings and other supplementary information.
❗	Important notes provide information on required configuration settings and other critical information.
💡	Tips provide recommendations or alternative methods of performing tasks or configuring settings.
⚠	Warnings provide information that, when ignored, may result in potential loss, injury, or even death.

2. Product Overview

This chapter provides basic information about the QNAP device.

About the QHora-301W

The QHora-301W is QNAP's first 802.11ax-enabled router that comes with dual 10 GbE ports. The router features built-in SD-WAN technology to support VPN deployment. The QHora-301W features eight internal 5dBi antennas, four 1 GbE ports, and supports wireless transfer speeds up to 3600 Mbps. You can deploy the router as a hub or edge using QuWAN, QNAP's software defined-WAN (SD-WAN) technology.

Hardware Specifications

Warning
If your QNAP product has hardware defects, return the product to QNAP or a QNAP-authorized service center for maintenance or replacement. Any attempt to repair or perform maintenance procedures on the product by you or an unauthorized third party invalidates the warranty.
QNAP is not responsible for any damage or data loss caused by unauthorized modifications and installation of unsupported third-party applications.
For details, see the QNAP Warranty Terms and Conditions.

Tip
Model specifications are subject to change without prior notice. To see the latest specifications, go to https://www.qnap.com.

Component	QHora-301W
Processor	
CPU	Qualcomm® IPQ8074A Hawkeye 2
Frequency	4-core 2.2 GHz
Architecture	ARM Cortex-A53
Memory	1 GB RAM
Flash memory	4 GB eMMC
Network	
Gigabit network interface	• 2 x 10 GbE RJ45 • 4 x 1 GbE RJ45
Antenna	8 x 5dBi internal antennas
Total power consumption	24W
External I/O Ports & Expansion Slots	
USB ports	2 x USB 3.2 Gen 1 Type-A
Interface	
Buttons	• Reset • WPS
Switches	Power
Dimensions	
Dimensions (H x W x D)	250 × 180 × 48 mm (9.84 x 7.08 x 1.88 in)

Component	QHora-301W
Net weight	1.9 kg (4.18 lbs)
Other	
Operating temperature	0˚C to 40˚C (32˚F to 104˚F)
Relative humidity	Non-condensing relative humidity: 5% to 95%
Mount support	75 x 75 mm VESA mount (2.95 x 2.95 in)

Software Specifications

Specification	Description
System Status and Management	• Device connection status • Device health status • WAN status • Wireless status • Firmware schedule management
Wired Network Management	• Recommended WAN port configurations and usage scenarios: • 1GbE-1 port • 10GbE-1 port • 1GbE-1 and 1GbE-2 ports • WAN/LAN port configuration • Network port connection status • IEEE 802.1Q virtual LAN (VLAN) • IPv4 address routing management
Security	• Protocol-based firewall (TCP, UDP, ICMP, TCP+UDP) • IP address-based firewall rule configuration • Network Address Translation (NAT) and port forwarding
VPN	• Remote access support using L2TP, OpenVPN, QBelt (QNAP proprietary VPN), and WireGuard protocols • Client IP pool management • VPN client management • Connection logs • Maximum VPN tunnels: 30 (including QuWAN and QVPN connections)
Access Control	• Parental controls • Website filter and safe search

Specification	Description
System Settings	• Backup and restore • Restart, reset • Manage audio alerts • Local account and QNAP ID management • USB settings: USB device user management, USB usage overview, FTP server management
QuWAN	Configure organization, region, site, device name, and device role

Wireless Specifications

Specification	Description
Standards	• IEEE 802.11ax/ac/n/a 5 GHz • IEEE 802.11n/b/g 2.4 GHz
Operating Frequency	2.4 GHz, 5 GHz
Speeds	AX3600 • 5 GHz (2475 Mbps): 4 x 4 (80 MHz), 2 x 2 (160 MHz) • 2 GHz (1182 Mbps): 4 x 4 (40 MHz)
Modes	• Router mode • Access point (AP) mode
Guest Wireless Network	• 1 x 5 GHz • 1 x 2.4 GHz
Encryption	• WPA (Wireless Protected Access) • WPA2-PSK • WPA-PSK + WPA2-PSK • WPA-Enterprise • WPA2-Enterprise

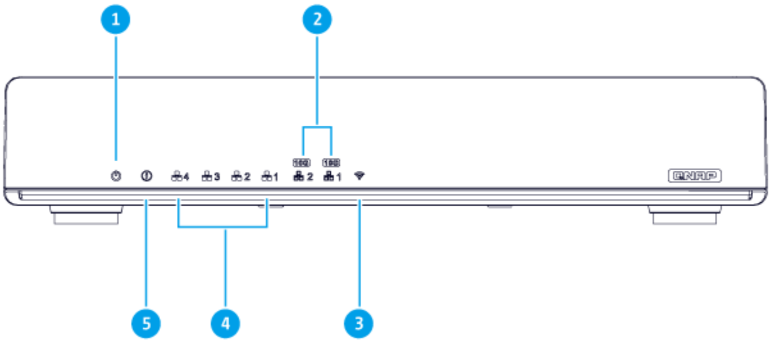
Specification	Description
Wireless Network Management	• Supports IEEE 802.11ax • Supports MU-MIMO technology • Supports band steering for dual-band (2.4 GHz and 5 GHz band) access points • Transmission power (high, middle, and low) • 20/40/80/160 MHz bandwidth • Auto and custom DFS (Dynamic Frequency Selection) channels • RTS/CTS (Request to Send/Clear to Send) functions • IEEE 802.3Q virtual LAN (VLAN) (Support for wired and wireless interface) • Smart connect • Supports IEEE 802.11r fast roaming • Wireless scheduler • Wireless Protected Setup (WPS)

Package Contents

Item	Quantity
QHora-301W router	1
AC power adapter	1
Ethernet cable	1

Components

Front Panel



No.	Component	No.	Component
1	Power LED	4	Gigabit Ethernet activity LEDs
2	10 Gigabit Ethernet Activity LEDs	5	Router status
3	Wireless LED	-	-

LEDs

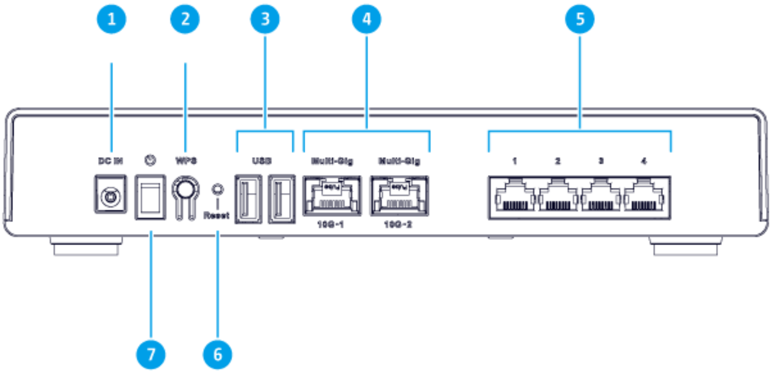
LEDs indicate the system status and related information when the device is powered on. The following LED information applies only when the drive is correctly installed and when the device is connected to the network or to a host.

For details on the location of the LEDs, see Components.

LED	Status	Description
Power	Green	The device is powered on.
System Status	Flashes green every 0.5 seconds	• The firmware is being updated. • The device is restarting. • The device is being initialized. • The device is locating another device.
	Green	The device is ready.
	Red	A system error occurred while powering on the device.

LED	Status	Description
Gigabit Ethernet activity	Green	A network connection has been established.
	Orange	WAN connection has been established.
10 Gigabit Ethernet (RJ45) activity	Green	A network connection has been established.
	Orange	WAN connection has been established.
Wireless	Green	Wireless connection has been established.
	Orange	Press the WPS button for 3 seconds.

Rear Panel



No.	Component	No.	Component
1	Power input	5	Gigabit Ethernet ports (RJ45)
2	WPS button	6	Reset button
3	USB 3.2 Gen 1 Type-A ports	7	Power switch
4	10 Gigabit Ethernet ports (RJ45)	-	-

Power Switch

Operation	User Action	Result
Power on	Move the power switch to the on position	The device powers on.
Power off	Move the power switch to the off position	The device powers off.

Reset Button

QNAP routers can be reset to factory defaults using the reset button located on the rear side of the device.

For details on the component placement, see the rear side of the device (see Rear Panel).

Operation	User Action	Result
Reset	Press and hold the button for 10 seconds	The router resets and all default settings are restored. This will clear any statically assigned IP address information, WAN and LAN configurations, and security settings. The router is unbound from the QNAP ID.

Safety Information

The following instructions help ensure personal safety and environmental safety. Read these instructions carefully before performing any operations.

General Instructions

- The device should be stored in a secure location with restricted access, controlled through the use of a tool, lock and key, or any means of security.
- Only qualified, skilled, and authorized persons with knowledge of all restrictions, safety precautions, and installation and maintenance procedures should have physical access to the device.
- To avoid potential injury or damage to components, ensure that the drives and other internal system components have cooled before touching them.
- Observe electrostatic discharge (ESD) procedures to avoid potential injury or damage to components.

Power

- To reduce the risk of fire or electric shock, ensure that you only connect the power cord to a properly grounded electrical outlet.
-

  Devices with redundant power supply may have one or more power supply unit (PSU) cords. To avoid serious injuries, a trained service technician must disconnect all PSU cords from the device before installing or replacing system components.

3. Installation and Access

This chapter provides specific hardware installation and router access steps.

Installation Requirements

Category	Item
Environment	• Room temperature: 0˚C to 40˚C (32˚F to 104˚F) • Non-condensing relative humidity: 5% to 95% • Wet-bulb temperature: 27˚C (80.6˚F) • Flat, anti-static surface without exposure to direct sunlight, liquids, or chemicals
Hardware and peripherals	Network cable
Tools	Anti-static wrist strap

Setting Up the Router

1. Place your router in an environment that meets the requirements.
   For details, see Installation Requirements.

2. Power on the router.
   For details, see Rear Panel.

3. Check if the power LED and system status LED are green.
   For details, see LEDs.

4. Connect the router to the network and the computer.
   For details, see Connecting the Router to the Internet.

5. Check if the WAN interface LED is orange and LAN interface LED is green.
   For details, see LEDs.

6. Log on to QuRouter with the local account credentials or QNAP ID.
   For details, see Binding the Router with a QNAP ID.

Connecting the Router to the Internet

1. Connect the power cord to the electrical outlet.

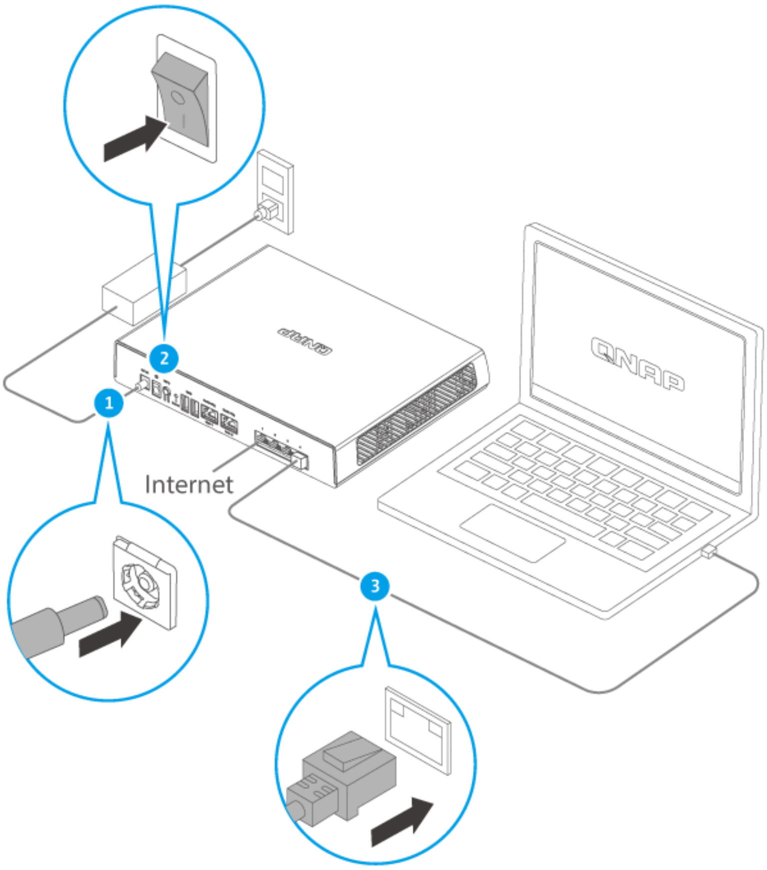
2. Power on the router.

3. Connect the router to the Internet.

    a. Connect the router to WAN interface.

    b. Connect an Ethernet cable to the 1 GbE port 1 interface on the router.

    c. Connect the Ethernet cable to the Ethernet port of the ISP gateway.



4. Connect the router to the computer.

    a. Connect an Ethernet cable to any other 1 GbE port on the router.

    b. Connect the Ethernet cable to a Gigabit Ethernet port on the computer.

5. Verify that the router is recognized by the computer.

    a. Open Qfinder Pro on the host computer.

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

    b. Locate the router on the list.

6. Open a web browser.

7. Enter http://192.168.100.1 to access the QuRouter web interface.

8. Follow the installation guide to configure the initial settings of QHora-301W.

Router Access

Method	Description	Requirements
Web browser	You can access the router using any computer on the same network if you have the following information: • Router IP address • Login credentials of a valid user account For details, see Accessing the Router Using a Browser.	• A computer connected to the same network as the router • Web browser
Qfinder Pro	Qfinder Pro is a desktop utility that enables you to locate and access QNAP devices on a specific network. The utility supports Windows, macOS, Linux, and Chrome OS. To download Qfinder Pro, go to https://www.qnap.com/utilities. For details, see Accessing the Router Using Qfinder Pro.	• A computer connected to the same network as the router • Web browser • Qfinder Pro

Accessing the Router Using a Browser

You can access the router using any computer on the network if you know the IP address and login credentials of a valid user account.

> **Note**
> You can use Qfinder Pro to locate the router IP address.

1. Verify that your computer is connected to the same network as the router.
2. Open a web browser on your computer.
3. Enter the IP address of the router in the address bar.
   The QuRouter web interface page appears.
4. Specify the default username and password.

Default Username	Default Password
`admin`	QuRouter: The router MAC address without any punctuation and all letters capitalized. **Tip** For example, if the MAC address is 00:0a:0b:0c:00:01, the default password is 000A0B0C0001.

5. Click **Login**.
   The QuRouter dashboard page appears.

Accessing the Router Using Qfinder Pro

Qfinder Pro is a desktop utility that enables you to locate and access QNAP devices on a specific network. The utility supports Windows, macOS, Linux, and Chrome OS.

1. Install Qfinder Pro on a computer that is connected to the same network as the router.
   To download Qfinder Pro, go to https://www.qnap.com/utilities.
2. Open Qfinder Pro.
   Qfinder Pro automatically searches for all QNAP devices on the network.
3. Locate the router in the list and then double-click the name or IP address.
   The default web browser page opens.
4. Specify the default username and password.

Default Username	Default Password
`admin`	QuRouter: The router MAC address without any punctuation and all letters capitalized. **Tip** For example, if the MAC address is 00:0a:0b:0c:00:01, the default password is 000A0B0C0001.

5. Click **Login**.
   The home page appears.

4. QuRouter

About QuRouter

QuRouter is a centralized management interface that comes with your QNAP router, accessible by visiting the router's IP address in a web browser. With its intuitive interface, QuRouter makes it easy to set up, secure, and configure the features of your router.

System Requirements

Category	Details
Hardware	A QNAP router
Software	• Web browser: • Microsoft Edge 42 or later • Mozilla Firefox 60.0 or later • Apple Safari 11.1 or later • Google Chrome 70.0 or later • Qfinder Pro 6.9.2 or later

Getting Started

1. Log on to QuRouter with the local account credentials or QNAP ID.
   For details, see Binding the Router with a QNAP ID.

2. Configure network settings.
   For details, see Changing WAN Port Configurations.

3. Configure wireless settings.
   For details, see the following topics:

   - Configuring Virtual Access Point Settings
   - Configuring the Guest Wireless Network
   - Configuring Wi-Fi Protected Setup (WPS)

4. Configure system settings.
   For details, see the following topics:

   - Editing the Device Name
   - Configuring Access Control Settings
   - Restart, Reset, Backup, and Restore
   - Enabling the Audio Alert Setting

5. Configure QVPN settings.
   For details, see the following topics:

   - Adding a QVPN User

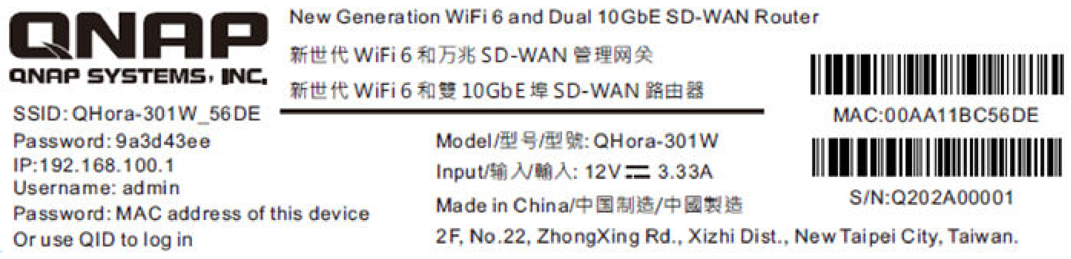
- Enabling a QBelt VPN Server
- Enabling an L2TP VPN Server
- Enabling an OpenVPN VPN Server

Configuring QuRouter

This sections explains how to configure the router using the web management interface during the initial setup process.

1. Open a web browser.
2. Enter `192.168.100.1` in the address bar.
   The QuRouter login screen appears.
3. Alternatively, use Qfinder Pro to locate the router on the list.
4. Double-click on the name or IP address.
   The **Smart Installation Guide** page appears.
5. Click **Start**.
   The local account password page appears.
6. Specify a new password for the local account.

> **Note**
> The default password is the router MAC address without any punctuation and all letters capitalized.
> For example, if the MAC address is 00:0a:0b:0c:00:01, the default password is 000A0B0C0001.



QNAP
QNAP SYSTEMS, INC.
New Generation WiFi 6 and Dual 10GbE SD-WAN Router
新世代 WiFi 6 和万兆 SD-WAN 管理网关
新世代 WiFi 6 和雙 10GbE 埠 SD-WAN 路由器
SSID: QHora-301W_56DE
Password: 9a3d43ee
IP:192.168.100.1
Username: admin
Password: MAC address of this device
Or use QID to log in
Model/型号/型號: QHora-301W
Input/输入/輸入: 12V ⎓ 3.33A
Made in China/中国制造/中國製造
2F, No.22, ZhongXing Rd., Xizhi Dist., New Taipei City, Taiwan.
MAC:00AA11BC56DE
S/N:Q202A00001

The MAC address can be found on the asset tag on the bottom of the device.

7. Click **Next**.
   The domain selection page appears.
8. Select the domain from the following.
   - **Global**
   - **China**
9. Click **Next**.
   The **WAN Settings** page appears.
10. Select one of the following WAN interface settings.

Setting	Description
DHCP	Obtain IP address settings automatically via DHCP

Setting	Description
Static IP	Manually assign a static IP address. You must specify the following information: • Fixed IP address • Subnet mask • DNS server
PPPoE	Select this option to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

11. Click **Apply**.

12. Specify the current location of the device.

    a. Click the drop-down list to select the country or region.

> **Note**
> If the selected location does not match with the IP geolocation of the device, a confirmation message appears prompting you to use the router in basic wireless mode.
> The basic wireless mode has the following limitations:
>
> - The 2.4GHz band only provides access to channels 1 - 11.
> - The 5 GHz bands are unavailable.
> - The 2.4 GHz band operates on low output power.

    b. Click **Apply**.
    QuRouter verifies the location of the device.

13. Update the firmware to the latest version.
    For details, see the Firmware section.

14. Click **Apply**.

15. Enter the default username and password.

Default Username	Default Password
`admin`	QuRouter: The router MAC address without any punctuation and all letters capitalized. **Tip** For example, if the MAC address is 00:0a:0b:0c:00:01, the default password is 000A0B0C0001. The MAC address can be found on the asset tag on the rear side of the device.

16. Click **Login**.
    The **Local Account** window appears.

17. Optional: You can log in to QuRouter using your QNAP ID and password.
    For details, see Binding the Router with a QNAP ID.

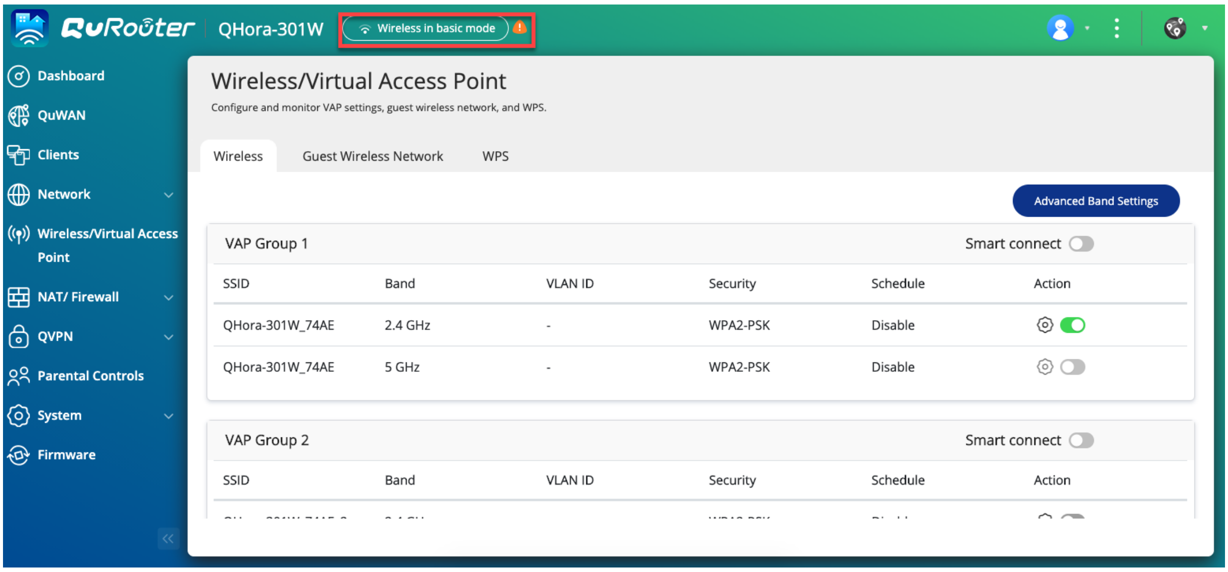
18. Reenter or modify the local account username and password.

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

QuRouter saves the settings.

Enabling the Full Wireless Functionality in QuRouter

1. Log in to QuRouter.
2. Click **Basic Wireless Mode**.



Wireless/Virtual Access Point

Configure and monitor VAP settings, guest wireless network, and WPS.

VAP Group 1

SSID	Band	VLAN ID	Security	Schedule	Action
QHora-301W_74AE	2.4 GHz	-	WPA2-PSK	Disable	
QHora-301W_74AE	5 GHz	-	WPA2-PSK	Disable	

VAP Group 2

SSID	Band	VLAN ID	Security	Schedule	Action

The **Wireless Regulatory Domain Settings** page appears.

3. Select the current location of the device.
4. Click **OK**.

QuRouter enables all the wireless functions of the router.

Binding the Router with a QNAP ID

1. Log in to QuRouter with your QNAP ID and password.

Note
To create a new QNAP account, click **Create Account**.

2. Click **Login**.
   The **Local Account** window appears.
3. Enter the local account credentials in order to complete the 2-step verification process.
4. Click **OK**.
   The QuRouter dashboard opens and the **Edit Device Name** window appears.
5. Specify a device name containing between 3 to 15 alphanumeric characters.
6. Click **OK**.

The router is bound to the QNAP ID.

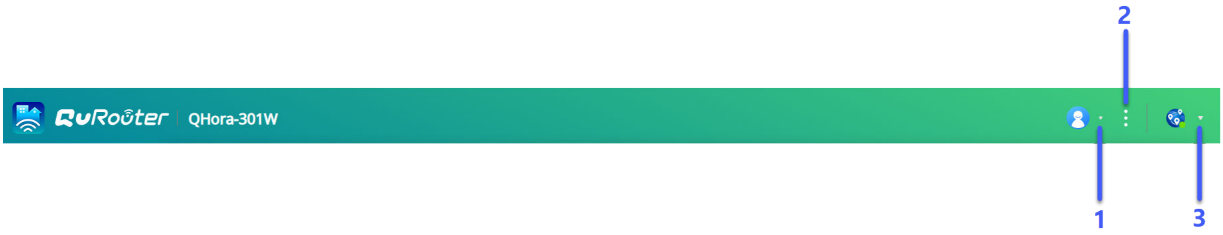
Unbinding the Router from a QNAP ID

1. Log in to QuRouter.
2. Go to **System** > **Access Control** > **Administrator** .
3. Below **Unbind QNAP ID**, click 🗑.
   A confirmation message appears.
4. Click **OK**.

Note
The router is unbound from the QNAP ID and you are logged out of QuRouter.

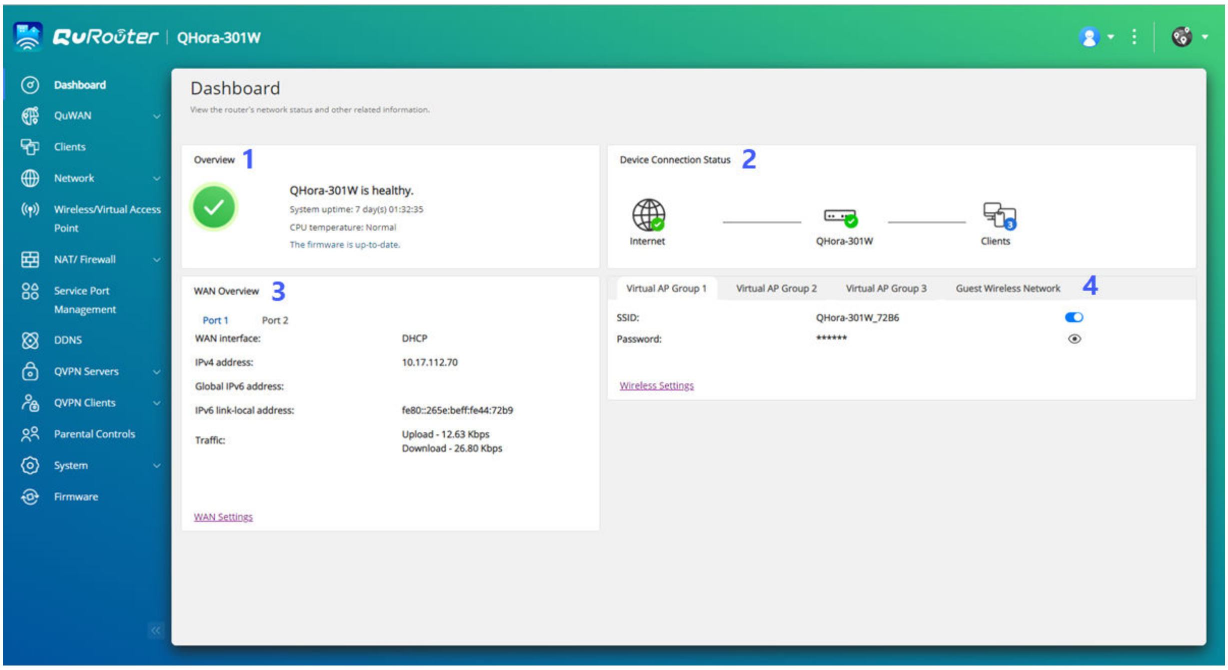
5. QuRouter Navigation

Taskbar



No.	Element	User Action
1	**[USER_NAME]**	**Logout**: Logs the user out of the current session
2	**More**	Click the button to view the following menu items: • **Language**: Opens a list of supported languages and allows you to change the language of the operating system • **Domain Settings**: Click to change the domain. **Note** You cannot change the domain if the router was previously added to the QuWAN network. • **About**: Displays the following information: • Operating system • Hardware model • Firmware version • **QNAP Remote Support**: Click to create a support ticket and contact the QNAP Customer Service team. For details, see Using QNAP Remote Support to Resolve Router Issues.
3	QuWAN	Click the button to view QuWAN-related information. • QuWAN Orchestrator connection status • Organization • QuWAN settings • Link to QuWAN Orchestrator

Dashboard



Dashboard

View the router's network status and other related information.

Overview

QHora-301W is healthy.

System uptime: 7 day(s) 01:32:35

CPU temperature: Normal

The firmware is up-to-date.

Device Connection Status

WAN Overview

Port 1 Port 2

WAN interface:	DHCP
IPv4 address:	10.17.112.70
Global IPv6 address:	
IPv6 link-local address:	fe80::265e:beff:fe44:72b9
Traffic:	Upload - 12.63 Kbps Download - 26.80 Kbps

WAN Settings

SSID:	QHora-301W_72B6
Password:	******

Wireless Settings

No.	Section	Displayed Information	User Action
1	Overview	• Uptime (number of days, hours, minutes and seconds) • CPU temperature • Firmware information	-
2	Device Connection Status	• Internet status • Device status • Number of connected clients	-
3	WAN Overview	• Port information • WAN interface • IPv4 address • Global IPv6 address • IPv6 link-local address • Traffic	Click **WAN Settings** to open **Network** > **WAN & LAN Settings** .

No.	Section	Displayed Information	User Action
4	Virtual Access Point Groups	Virtual Access Groups/ Guest Wireless Network • SSID • Password	• Click **Wireless Settings** to open the wireless settings page. • Click ● to enable a VAP group or guest wireless network. **Tip** Click 👁 to make the password visible.

6. System Configuration

System

Configuring Router Operation Modes

QuRouter provides access to two router operation modes.

- **Wireless router**: The default router mode where the device can connect to the internet and share the wireless network with its client devices. NAT and DHCP are enabled by default.
- **Access point (AP)**: The router connects to another wireless router using a network cable to extend the coverage of the wireless signal to other network devices. Router-related features (DHCP server, NAT, QuWAN, and WAN) are disabled when the router operates as a wireless access point.
  For details on configuring access point mode, see Configuring Access Point (AP) Mode.

1. Log in to QuRouter.
2. Go to **System** > **Operation Mode** .
3. Select a router operation mode.
4. Click **Apply**.

QuRouter applies the operation mode settings.

Configuring Access Point (AP) Mode

Access point (AP): The router connects to another wireless router using a network cable to extend the coverage of the wireless signal to other network devices. Router-related features (DHCP server, NAT, QuWAN, and WAN) are disabled when the router operates as a wireless access point.

1. Log in to QuRouter.
2. Go to **System** > **Operation Mode** .
3. Select **Access point (AP) mode**.
   a. Optional: Select **Enable Spanning Tree Protocol (STP)**.
   b. Select one of the following IP allocation methods:
      - **DHCP**: Obtains the IP address information automatically from the DHCP server.
      - **Static IP**: Specify the IP address information manually.
        Configure the following static IP address 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.
Default gateway	Specify the IP address of the default gateway for the DHCP server.
DNS server	Specify a DNS server for the DHCP server.

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

5. Click **OK**.

> **Important**
> The following settings are changed when the router is switched to AP mode.
>
> - The router is unbound from the QNAP ID.
> - The router is removed from the QNAP organization and QuWAN. You must reconfigure the QuWAN settings if you enable the router mode again.

6. Run Qfinder Pro on a computer connected to the same local area network.

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

7. Locate the router in the list and double-click the name or IP address.
   The login screen appears.

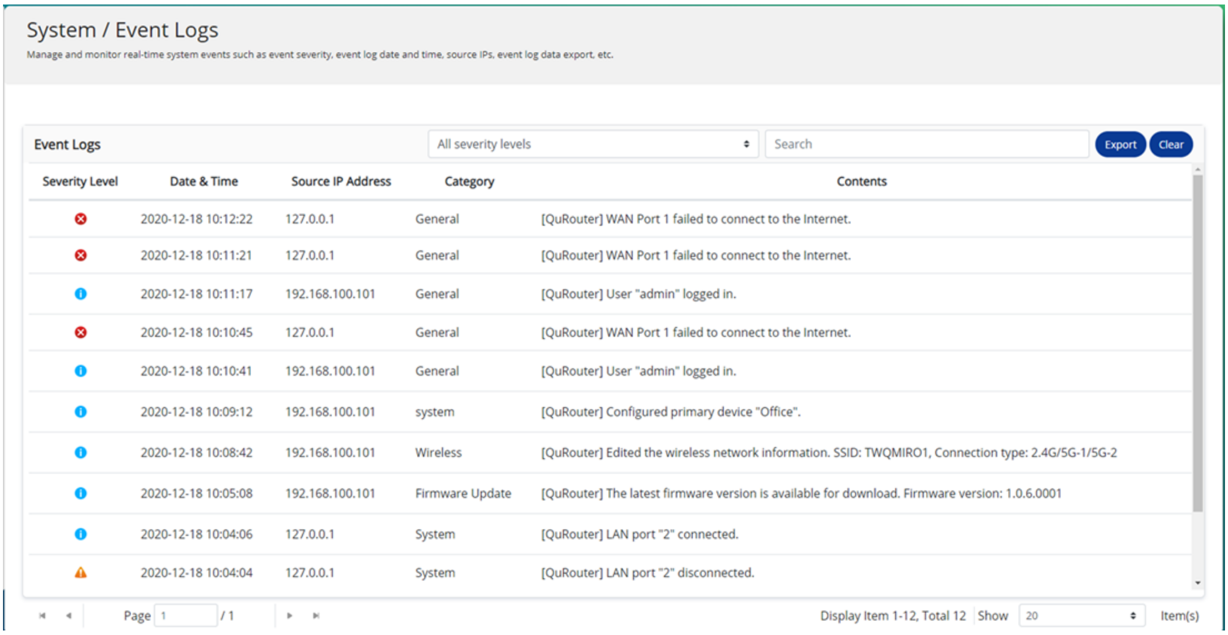
8. Enter the local account credentials of the router.

9. Click **Login**.

> **Note**
> QuRouter displays only information related to access point settings such as network, wireless, firmware, and system settings.

Managing Event Logs

You can view a record of event logs related to the router by going to **System** > **Event Logs** . Common events include enabling or disabling network services, configuring account and system settings, and configuring security settings.



System / Event Logs

Manage and monitor real-time system events such as event severity, event log date and time, source IPs, event log data export, etc.

Event Logs

All severity levels

Search

Severity Level	Date & Time	Source IP Address	Category	Contents
⊗	2020-12-18 10:12:22	127.0.0.1	General	[QuRouter] WAN Port 1 failed to connect to the Internet.
⊗	2020-12-18 10:11:21	127.0.0.1	General	[QuRouter] WAN Port 1 failed to connect to the Internet.
ⓘ	2020-12-18 10:11:17	192.168.100.101	General	[QuRouter] User "admin" logged in.
⊗	2020-12-18 10:10:45	127.0.0.1	General	[QuRouter] WAN Port 1 failed to connect to the Internet.
ⓘ	2020-12-18 10:10:41	192.168.100.101	General	[QuRouter] User "admin" logged in.
ⓘ	2020-12-18 10:09:12	192.168.100.101	system	[QuRouter] Configured primary device "Office".
ⓘ	2020-12-18 10:08:42	192.168.100.101	Wireless	[QuRouter] Edited the wireless network information. SSID: TWQMIRO1, Connection type: 2.4G/5G-1/5G-2
ⓘ	2020-12-18 10:05:08	192.168.100.101	Firmware Update	[QuRouter] The latest firmware version is available for download. Firmware version: 1.0.6.0001
ⓘ	2020-12-18 10:04:06	127.0.0.1	System	[QuRouter] LAN port "2" connected.
⚠	2020-12-18 10:04:04	127.0.0.1	System	[QuRouter] LAN port "2" disconnected.

Page 1 / 1

Display Item 1-12, Total 12 Show 20 Item(s)

System Settings

Editing the Device Name

1. Log in to QuRouter.
2. Go to **System** > **System Settings** > **Device Name Settings** .
3. Click ✎ .
   The **Edit Device Name** window appears.
4. Specify device name that consists of 3 to 15 characters from any of the following group:
   Valid characters: A–Z, a–z, 0–9
5. Click **OK**.

QuRouter updates the device name.

Restart, Reset, Backup, and Restore

QuRouter system settings allows you to remotely control the restart, reset, backup, and restoration operations of the router.

Restarting the Router

1. Go to **System** > **System Settings** > **Restart / Reset / Backup / Restore** .
2. Click **Restart**.
   A confirmation message appears.
3. Click **OK**.

QuRouter restarts the device.

Resetting the Router

1. Go to **System** > **System Settings** > **Restart / Reset / Backup / Restore** .
2. Click **Reset**.
   A confirmation message appears.
3. Click **I agree**.
4. Click **OK**.

QuRouter resets the device to default settings and the router is unbound from QNAP ID.

Backing Up System Settings

1. Go to **System** > **System Settings** > **Restart / Reset / Backup / Restore** .
2. Click **Backup**.

The 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 existing information.

1. Go to **System** > **System Settings** > **Restart / Reset / Backup / Restore** .
2. Under **Restore**, click **Browse**.
   A file explorer window opens.
3. Select a valid BIN file that contains the device system settings.
4. Click **Restore**.

QuRouter restores the router settings.

Enabling the Audio Alert Setting

1. Log in to QuRouter.
2. Go to **System** > **System Settings** > **Audio Alert** .
3. Click ○ .
   QuRouter enables audio alerts on the router.

Configuring Access Control Settings

Access Control settings can control how devices connect to the router. These settings can help increase network security and minimize security threats.

1. Log in to QuRouter.
2. Go to **System** > **Access Control** > **Access Control Settings** .
3. Enable the access control settings.

Setting	User Action
Local management via HTTP	Enable to allow local access to the router web interface using non-HTTPS connections. **Note** HTTP connections are faster than Hypertext Transfer Protocol Secure (HTTPS); however, the transferred content is not encrypted.
Remote management	Enable to allow administrators remote access to the router web interface via the WAN IP address.

Configuring Local Account Settings

> **Note**
> The administrator account is the default router account. You cannot delete the administrator account.

1. Log in to QuRouter.
2. Go to **System** > **Access Control** > **Administrator** .
3. Click ✎ to configure local account credentials.
The **Local Account** window appears.
4. Configure the local account settings.

Description	User Action
Username	Specify a username that contains 5 to 32 characters. Valid characters: A–Z, a–z, 0–9
Current password	Enter the current password of the local account.
New password	Specify a password that contains 8 to 64 ASCII characters.
Confirm new password	Enter the password again.

5. Click **OK**.

QuRouter updates the local account settings.

USB Settings

The **System** > **USB Settings** page allows you to access and manage USB-related settings, FTP access, and FTP users.

Configuring FTP Access

1. Log in to QuRouter.
2. Go to **System** > **USB Settings** > **FTP Settings** .
3. Enable **FTP Server**.
4. Click ⚙.
The **FTP Settings** window appears.
5. Configure the FTP server settings.

Setting	User Action
Concurrent connections	Specify a number between 1 and 9. **Note** QuRouter allows up to 9 concurrent connections.
File name encoding	Select from the following options: • **utf-8** • **big5**

6. Click **Save**.
QuRouter saves the FTP settings.

Note
Click the external link IP address to access the contents of the USB device connected to the router if you are accessing the network through the WAN port.
Click the internal link IP address to access the contents of the USB device connected to the router if you are accessing the network through the LAN port.

Adding an FTP User

1. Log in to QuRouter.
2. Go to **System** > **USB Settings** > **FTP Settings** .
3. Click **Add FTP User**.
   The **Add FTP User** window appears.
4. Configure the FTP user settings.

Setting	User Action
Username	Enter a username that contains 5 to 32 characters. Valid characters: A–Z, a–z, 0–9
Password	Specify a password that contains 8 to 63 characters. **Note** • Passwords are case-sensitive. • Click 👁 to make the password visible.

5. Click **Add**.

QuRouter saves the FTP user information.

Configuring an FTP User

1. Log in to QuRouter.
2. Go to **System** > **USB Settings** > **FTP Settings** .
3. Identify an FTP user to configure.
4. Click ✎ .
   The **Edit FTP User** window appears.
5. Configure FTP user settings.
   For details, see Adding an FTP User.
6. Click **Edit**.

QuRouter updates the FTP user information.

Deleting an FTP User

1. Log in to QuRouter.
2. Go to **System** > **USB Settings** > **FTP Settings** .

3. Identify an FTP user you want to delete.
4. Click 🗑.
   A confirmation message appears.
5. Click **OK**.

QuRouter deletes the FTP user.

Capturing Traffic Packets Using a USB Device

You can analyze network traffic and troubleshoot network issues using the packet capture utility built into the USB interface of the router. Connect a USB device to the router and capture data packets traveling over the network for monitoring and recording purposes.

1. Log in to QuRouter.
2. Go to **System** > **USB Settings** > **USB Packet Capture** .
3. Configure the settings.

Setting	User Action
USB port	Select the USB interface.
File name	Specify a target file name between 1 and 64 characters. Valid characters:: A–Z, a–z, 0–9, Hyphen (-), Underscore (_) **Note** The .pcap file is automatically stored in the USB device that is connected to the router.
Duration	Select a capture time from the drop-down menu.
Interface	Select a network interface used to capture packet data.

4. Configure the filter settings.

Setting	User Action
Source IP addresses	Specify an IP address used to send data.
Source port	Specify a port number used to send data.
Destination IP addresses	Specify an IP address used to receive data.
Destination port	Specify a port number used to receive data.

5. Click **Start**.

QuRouter starts capturing data packets to the USB device.

Firmware

QNAP recommends keeping your router firmware up to date. This ensures that your router can benefit from new features, enhancements, and bug fixes.

Checking for Live Updates

1. Go to **Firmware**.

2. Enable **Live update**.
3. Select one or more of the following options:
    - **Update now**
    - **Schedule update at**

Note
Select the date and time to schedule the firmware update.

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

QuRouter checks for firmware updates.

Updating the Firmware Manually

The update may require several minutes or longer, depending on your hardware configuration and network connection.

1. Download the router firmware.
2. Go to http://www.qnap.com/download.
    a. Select your router model.
    b. Read the release notes and confirm the following:
        - The router model matches the firmware version.
        - Updating the firmware is necessary.
    c. Ensure that the product model and firmware are correct.
    d. Download the firmware package.
    e. Extract the firmware package file.
3. Go to **Firmware**.
4. Select **Manual update**.
5. Click **Browse** and then select the extracted firmware package file.
6. Click **Apply**.

The device is immediately restarted.

7. Network Settings

Network

Changing WAN Port Configurations

1. Log in to QuRouter.
2. Go to **Network** > **WAN & LAN Settings** .
3. Select the WAN port configuration from the following options based on your network requirements.

Setting	User Action
WAN 1 GbE port 1	Select to build a high-speed 10 GbE intranet by connecting 2 x 10 GbE ports to 10 GbE devices in a LAN environment and connecting the 1 GbE port 1 interface to the WAN interface.
WAN 10 GbE port 1	Select to configure a high-speed interoffice VPN network by connecting the 10 GbE port 1 interface to the WAN interface and connecting the 10 GbE port 2 interface to a server or storage device in a LAN environment.
WAN 1 GbE port 1 and 1 GbE port 2	Select to configure an SD-WAN environment (QuWAN) by connecting 2 x 1 GbE ports to the WAN interface and connecting 2 x 10 GbE ports to server or storage devices in a LAN environment.

A confirmation message appears.

4. Click **Apply**.

Important
Updating the WAN port configuration automatically deletes all the port forwarding rules.

QuRouter updates the WAN port configuration.

Configuring Wide Area Network (WAN) Interface Settings

1. Log in to QuRouter
2. Go to **Network** > **WAN & LAN Settings** .
3. Identify a WAN interface.
4. Click ⚙.
   The port configuration window appears.
5. Configure the IPv4 settings.
   a. Select the WAN interface setting from the following options.

Setting	Description
DHCP	Obtain IP address settings automatically via DHCP

Setting	Description
Static IP	Manually assign a static IP address. You must specify the following information: • Fixed IP Address • Subnet Mask • Default Gateway • DNS Server
PPPoE	Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

b. Configure the DNS settings.

Setting	Description
DNS server	Select from the following: • **Auto**: Automatically obtain the IP address using DHCP. • **Manually**: Manually assign the IP address for the primary and secondary DNS servers. **Important** QNAP recommends specifying at least one DNS server to allow URL lookups.

c. Specify a port description.

d. Specify an MTU value between 576 and 1500.

e. Specify the transferring and receiving ISP line rate.

> **Note**
> You can set the ISP line rate only if you have configured the QuWAN and QoS settings.

6. Configure the IPv6 settings.

a. Click **IPv6**.

b. Select the WAN interface.

Setting	User Action
DHCPv6	The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server. **Important** This option requires an available DHCPv6-enabled server on the network.

Setting	User Action
Static IP	Manually assign a static IP address to the adapter. You must specify the following information: • Fixed IP Address • Prefix length **Tip** Obtain the prefix length information from your network administrator. • Default Gateway • Primary and secondary DNS servers
PPPoEv6	Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE) IPv6 protocol. **Important** You must change the IPv4 WAN interface to PPPoE if you want to use PPPoEv6 as the WAN interface.
Stateless (SLAAC)	The adapter automatically acquires an IPv6 address and DNS settings from the router. **Important** This option requires an available IPv6 RA (router advertisement)-enabled router on the network.

c. Configure the DNS settings.

7. Click **Apply**.

QuRouter updates the WAN settings.

Configuring Local Area Network (LAN) Access and Trunk Modes

Access mode is used in environments without any user-configured VLANs. This mode allows the router to carry traffic without VLAN tagging and is used to connect end-user devices such as laptops, NAS, or printers.

Trunk mode is used in a VLAN-configured environment and is designed for connecting devices operating on tagged VLANs (for example, VLAN-enabled switch, VLAN-enabled NIC, etc.). Ports using Trunk mode can be linked between various network devices and are capable of carrying traffic across multiple VLANs. A VLAN must be configured prior to configuring Trunk mode on the LAN port.

1. Log in to QuRouter.
2. Go to **Network** > **WAN & LAN Settings** .
3. Identify a LAN port.
4. Under Action, click ⚙.
   The port configuration window appears.
5. Configure the mode settings.

Setting	User Action
Mode	Select from the following options: • **Access mode** • **Trunk mode**: Select one or more VLANs from the VLAN list to enable trunk mode. **Tip** To create a new VLAN, see Adding a VLAN.
Description	Enter a description for the port.

6. Click **OK**.

QuRouter updates the LAN port mode.

Locating Other QNAP Devices on the Network

The QHora-301W can find other QNAP devices connected to the same network subnet.

1. Log in to QuRouter.
2. Go to **Connected QNAP Devices**.
3. You can perform the following actions.

Task	Possible User Action
Locate a device	**a.** Type the keywords in the search field. **b.** Press **Enter**.
Copy the device IP or MAC address	Beside the IP or MAC address, click ⧉ .
Refresh the device list	Click ⟳.

VLAN

A virtual LAN (VLAN) groups multiple network devices together and limits the broadcast domain. Members of a VLAN are isolated and network traffic is only sent between the group members. You can use VLANs to increase security and flexibility while also decreasing network latency and load.

The VLAN screen displays information about existing VLANs and provides access to VLAN configuration options.

Adding a VLAN

1. Log in to QuRouter.
2. Go to **Network** > **VLAN & DHCP Server Service Settings** .
3. Click **Add VLAN**.
   The **Add VLAN** window opens.
4. Configure the IPv4 VLAN settings.
   a. Specify a VLAN ID.

b. Specify a VLAN description that contains a maximum of 256 characters.

c. Specify a fixed IP address.

d. Specify the subnet mask.

e. Specify an MTU value.

f. Select **Enable Spanning Tree Protocol (STP)** to prevent bridge loops.

g. Select **Enable DHCP server service**.
Configure DHCP settings.

Field	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
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.
Reserved IP Table	**1.** Click **Add** to configure a reserved IP table. **2.** Specify the following: • Device name • IP address • MAC address **3.** Click ✓.

5. Configure the IPv6 VLAN settings.

a. Click **IPv6**.

b. Click **Enable IPv6 VLAN**.

c. Select the outgoing WAN interface from the drop-down list.

d. Specify the IPv6 IP address prefix.

e. Select the prefix length from the drop-down list.

f. Select the interface identifier to identify interfaces on a link.

Setting	User Action
Interface identifier	Select from the following: • **EUI-64**: Select Extended Unique Identifier (EUI-64) to automatically configure IPv6 host address. • **Manually**: Specify an interface ID to configure the IPv6 host address.

g. Assign a client IPv6 addressing mode from the drop-down list.

Setting	Description
IPv6 addressing mode	Select from the following: • **Stateful**: The stateful DHCPv6 or managed mode enables you to manually assign a unique IPv6 address to each client. • **Stateless**: The stateless DHCPv6 mode enables users to manually enter additional IPv6 information including the lease time, but automatically assigns a unique IPv6 address to each client. • **SLAAC+RDNSS**: Stateless Address Auto-Configuration (SLAAC) along with Recursive DNS Server (RDNS) enables users to manually assign an IP address based on the IPv6 prefix and uses recursive queries to resolve the domain name. • **Disabled**: Disables IPv6 client addressing.

6. Click **Apply**.

QuRouter adds the VLAN.

Configuring VLAN Settings

1. Log in to QuRouter.
2. Go to **Network** > **VLAN & DHCP Server Service Settings** .
3. Identify a VLAN to configure.
4. Click ⚙.
   The **VLAN Configuration** window opens.
5. Edit the VLAN settings.

Note
To configure the VLAN settings, see Adding a VLAN.

6. Click **Apply**.

QuRouter updates the VLAN settings.

Deleting a VLAN

1. Log in to QuRouter.
2. Go to **Network** > **VLAN & DHCP Server Service Settings** .
3. Identify the VLAN.
4. Click 🗑.

Note
You cannot delete the VLAN if it being utilized by a WAN or LAN port.

A confirmation message appears.

5. Click **Delete**.

QuRouter deletes the VLAN.

Static Route

You can create and manage static routes in the **Static Route** section of network settings. Under normal circumstances, QuRouter 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.

You can view the IPv4 and IPv6 routing information in the following pages:

- IPv4 routing information: **Network** > **Routing** > **IPv4 / Routing Table**
- IPv6 routing information: **Network** > **Routing** > **IPv6 / Routing Table**

Routing tables provide status information regarding configured route entries from the following sources:

- Directly connected networks
- Dynamic routing protocols
- Statically configured routes

Adding an IPv4 Static Route

1. Log in to QuRouter.
2. Go to **Network** > **Routing** > **IPv4 / Static Route** .
3. Click **Add Static Route**.
   The **Add Static Route** window appears.
4. Configure the settings.

Setting	User Action
Destination	Specify a static IP address where connections are routed to.
Subnet Mask	Specify the IP address of the destination's subnet mask.
Next Hop	Select from the following next hop options: • **WAN Port**: Select an available WAN port IP address for the routing path. • **IP Address**: Specify the IP address of the closest or most optimal router in the routing path.
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.
Description	Enter a description for the static route.

5. Click **Apply**.

QuRouter creates the IPv4 static route.

Adding an IPv6 Static Route

1. Log in to QuRouter.
2. Go to **Network** > **Routing** > **IPv6 / Static Route** .
3. Click **Add Static Route**.
   The **Add Static Route** window appears.
4. Configure the settings.

Setting	User Action
Destination	Specify a static IP address where connections are routed to.
Prefix length	Select the prefix length for IPv6 addressing.
Next Hop	Select from the following next hop options: • **WAN Port**: Select an available WAN port IP address for the routing path. • **VLAN / Access mode**: Select a preconfigured access mode VLAN ID.
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.
Description	Enter a description for the static route.

5. Click **Apply**.

QuRouter creates the IPv6 static route.

Configuring a Static Route

1. Log in to QuRouter.
2. Select a static route.
   - IPv4 static route: **Network** > **Routing** > **IPv4 / Static Route**
   - IPv6 static route: **Network** > **Routing** > **IPv6 / Static Route**
3. Identify a static route.
4. Click ✎.
   The **Edit Static Route** window appears.
5. Configure the static route settings.
   For details, see the following:
   - Adding an IPv4 Static Route
   - Adding an IPv6 Static Route
6. Click **Apply**.

QuRouter updates the static route settings.

Deleting a Static Route

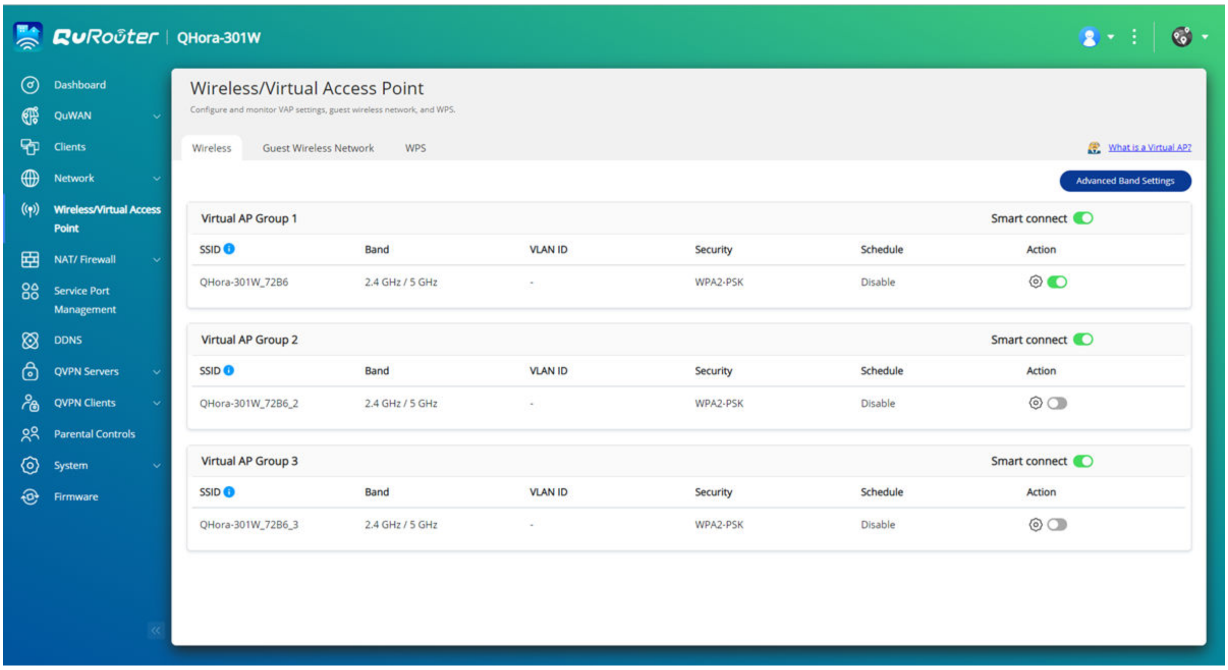
1. Log in to QuRouter.
2. Select a static route.
    - IPv4 static route: **Network** > **Routing** > **IPv4 / Static Route**
    - IPv6 static route: **Network** > **Routing** > **IPv6 / Static Route**
3. Identify a static route.
4. Click 🗑.
   A confirmation message appears.
5. Click **Apply**.

QuRouter deletes the static route.

Wireless/Virtual Access Points

Virtual Access Points

You can configure multiple virtual access groups from a single physical access point using virtual access points (APs). Each virtual AP group can be configured to control access to wireless devices and implement security protocols. This section controls the virtual AP settings, including Smart Connect, wireless scheduler, and security protocols.



Wireless/Virtual Access Point

Configure and monitor VAP settings, guest wireless network, and WPS.

Virtual AP Group 1 — Smart connect

SSID	Band	VLAN ID	Security	Schedule	Action
QHora-301W_72B6	2.4 GHz / 5 GHz	-	WPA2-PSK	Disable	

Virtual AP Group 2 — Smart connect

SSID	Band	VLAN ID	Security	Schedule	Action
QHora-301W_72B6_2	2.4 GHz / 5 GHz	-	WPA2-PSK	Disable	

Virtual AP Group 3 — Smart connect

SSID	Band	VLAN ID	Security	Schedule	Action
QHora-301W_72B6_3	2.4 GHz / 5 GHz	-	WPA2-PSK	Disable	

Configuring Virtual Access Point Settings

1. Go to **Wireless/Virtual Access Point** > **Wireless** .
2. Identify a virtual AP group to configure.

3. Optional: Enable **Smart Connect** to operate the access point using both 2.4 GHz and 5 GHz wireless bands.

> **Note**
> When enabled, Smart Connect uses the same SSID and password for both 2.4 GHz and 5 GHz bands.

4. Click ⚙.
   The **VAP Configuration** window appears.

5. Configure the virtual AP group settings.

Setting	User Action
VLAN ID	Select a VLAN ID from the drop-down list. **Note** To configure a new VLAN, go to Adding a VLAN.
SSID	Specify the virtual AP SSID.
Security	Select one of the following security authentication methods: • **WPA2-PSK** • **WPA-PSK / WPA2-PSK** • **WPA-Enterprise** • **WPA2-Enterprise** **Note** Enter a Remote Authentication Dial-In User Service (RADIUS) server IP address and server port number if the security authentication method is set to WPA-Enterprise or WPA2-Enterprise. • **WPA2-PSK / WPA3-Personal** • **OWE**
Password	Specify a password between 8 and 63 characters. **Note** The password is case-sensitive. **Tip** Click 👁 to make the password visible.
Enable 802.11r Fast Roaming	Select to enable the IEEE 802.11r or Fast BSS Transition (FT) to allow a wireless device to roam quickly in a network by pre-authenticating the device.
Enable Wireless Scheduler	You can select specific days and time periods to enable the virtual AP group.

6. Click **Apply**.

QuRouter updates the virtual AP group settings.

Configuring Advanced Band Settings on Virtual AP Groups

1. Go to **Wireless/Virtual Access Point** > **Wireless** .
2. Click **Advanced Band Settings**.
   The **Advanced Band Settings** window appears.
3. Configure the advanced settings for 5 GHz or 2.4 GHz bands.

Setting	User Action
Enable Band Steering	Enable to automatically reroute the wireless client to a wireless network that is utilizing the best frequency band available.
Enable MU-MIMO	Enable multiple-input, multiple-output technology (MU-MIMO) to allow the router to communicate concurrently with multiple wireless devices.
Transmission Power	Select one of the MU-MIMO transmission powers: • **High** • **Medium** • **Low**
Bandwidth	Specify one of the following frequencies: • **20 MHz** • **20/40 MHz** • **20/40/80 MHz** • **20/40/80/160 MHz** **Important** **20/40/80/160 MHz** is available only for the 5 GHz band.
Enable DFS Channels	Enable Dynamic Frequency Selection (DFS) to utilize more channels and avoid wireless interference. **Important** This setting is available only for the 5 GHz band.
Channels	Select the DFS channel that is less frequently used. **Note** The channel is set to **Auto** by default to avoid radio frequency interference.
Enable CTS/RTS	Specify a CTS/RTS value between 1 and 2347.

4. Click **Apply**.

QuRouter updates the advanced band settings.

Configuring the Guest Wireless Network

1. Go to **Wireless/Virtual Access Point** > **Guest Wireless Network** .
2. Select **Enable**.

3. Configure the guest wireless network settings.

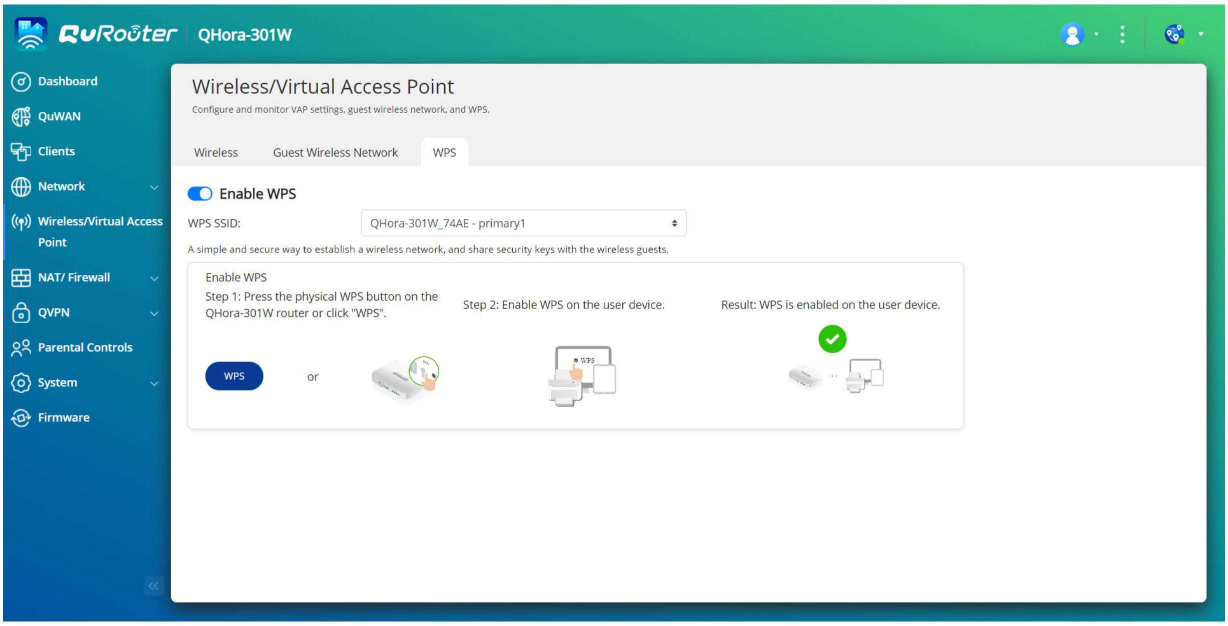
Setting	User Action
SSID	Specify a service set identifier (SSID) that can contain up to 32 characters. **Note** The SSID is case-sensitive.
Security	Select one of the following security authentication methods: • **WPA2-PSK** • **WPA-PSK / WPA2-PSK** • **WPA-Enterprise** • **WPA2-Enterprise** **Note** Enter a Remote Authentication Dial-In User Service (RADIUS) server IP address and server port number if the security authentication method is set to WPA-Enterprise or WPA2-Enterprise. • **WPA2-PSK / WPA3-Personal** • **OWE**
Password	Specify a password that contains 8 to 63 characters. **Note** The password is case-sensitive. **Tip** Click 👁 to make the password visible.

4. Click **Apply**.

QuRouter saves the guest wireless network settings.

Wi-Fi Protected Setup (WPS)

The WPS protocol is a standard that helps you easily set up a wireless network without needing to configure wireless network names (SSID) or security specifications.



Wireless/Virtual Access Point

Configure and monitor VAP settings, guest wireless network, and WPS.

Enable WPS

WPS SSID: QHora-301W_74AE - primary1

A simple and secure way to establish a wireless network, and share security keys with the wireless guests.

Enable WPS

Step 1: Press the physical WPS button on the QHora-301W router or click "WPS".

Step 2: Enable WPS on the user device.

Result: WPS is enabled on the user device.

Configuring Wi-Fi Protected Setup (WPS)

1. Go to **Wireless/ Virtual Access Point** > **WPS** .
2. Click ○ .
   QuRouter enables the WPS function.
3. Configure the WPS settings.

Option	Description
WPS SSID	Select the SSID from the drop-down menu.
WPS	Click **WPS** to enable WPS on the router. You can press the physical WPS button located on the rear panel of the router. **Note** For details, see Rear Panel

Clients

This section provides access to any wired or wireless clients connected to the router network.

Additionally, you can use the Blocked list to control the management of any clients blocked from accessing wired or wireless services.

Adding a Device to the Blocked List

1. Log in to QuRouter.
2. Go to **Clients** > **Blocked List** .
3. Click **Block client**.
   The **Add Device to Blocked List** window appears.
4. Configure the settings.

Setting	User Action
Description	Specify the device description. **Note** • The description must be between 1 to 20 characters. • Valid characters: A–Z, a–z, 0–9 • Valid special characters: Hyphen (-), Underscore (_), Period (.)
MAC Address	Specify the MAC address of the device.

5. Select the interface.
6. Click **Apply**.

QuRouter adds the device to the blocked list.

> **Tip**
>
> You can also block a client, by clicking ⊘ beside a client name in **Clients**.

Configuring a Device in the Blocked List

1. Log in to QuRouter.
2. Go to **Clients** > **Blocked List** .
3. Identity a device.
4. Click ✎.
   The **Edit Blocked List Device** window appears.
5. Configure the device settings.
   For details, see Adding a Device to the Blocked List.
6. Click **Apply**.

QuRouter updates the device information.

Deleting a Device from the Blocked List

1. Log in to QuRouter.
2. Go to **Clients** > **Blocked List** .
3. Identity a device.
4. Click 🗑.
   A confirmation message appears.
5. Click **Apply**.

QuRouter deletes the device from the blocked list.

SD-WAN

About QuWAN

QuWAN is a QNAP cloud-based SD-WAN networking solution that provides a centralized control platform to manage network functions of devices within its private network topology. QuWAN can intelligently and securely direct traffic across the WAN network.

You can configure the SD-WAN settings on the router and access QuWAN Orchestrator to manage the SD-WAN overlay network.

Configuring QuWAN Settings

1. Log in to QuRouter.

> **Note**
> If you are logging in with your QNAP ID for the first time, you are prompted to enter the local account credentials as part of the 2-step verification process.

> **Important**
> After configuring and saving the QuWAN settings, the device restarts to implement the settings and join the QuWAN network.

2. Go to **QuWAN** > **QuWAN Settings** .
3. Configure the QuWAN settings.

Setting	User Action
Organization	Select an organization associated with your QNAP ID. **Note** If there are no organizations associated with your QNAP ID, click **Create or edit organization**. QuRouter redirects you to QNAP Account website where you can create a new organization or edit an existing one.
Region	Select a region linked with the selected organization. Click **Add Region** to create a new region.
Site	Select a site from the drop-down menu. **Note** Click **Create or edit site** to create a new site associated with the selected organization or edit an existing site.
Device name	Specify a unique device name that consists of 3 to 15 characters from any of the following group. Valid characters: A–Z, a–z, 0–9

Setting	User Action
Device role	Select one of the following: • **Hub**: Configure the device as an SD-WAN hub. A public IP address is required for the WAN connection to select the device as a hub. • **Edge**: Configure the device as an SD-WAN edge. **Important** • You can only assign the device role of edge to devices behind NAT in an organization. • QuWAN Orchestrator automatically assigns the role of a hub to the first device added to the organization only if it is assigned a public IP address. • If the QuWAN device is using a private IP address, you can only assign the device role of edge using QuRouter. If you have enabled port forwarding on the router in front of the QuWAN device, you can change the device role from edge to hub in QuWAN Orchestrator.
Location	Select one of the following: • **Locate by IP address** • **Update by GPS coordinates**

4. Click **Join the Organization and QuWAN**.

> **Important**
>
> - The router is unbound from the QNAP ID once it is part of the QuWAN topology.
> - A QNAP router can support up to 30 VPN tunnels.

   A confirmation message appears.

5. Click **OK**.

QuRouter adds the router to the QuWAN topology.

Accessing QuWAN Orchestrator

1. Log in to QuRouter.
2. Click 🌐 located on the taskbar.
3. Click **Go to QuWAN Orchestrator**.
   QuWAN Orchestrator opens in a new browser tab.

Configuring the QuWAN QBelt VPN Server Settings

QNAP allows you to use QuWAN Orchestrator to configure your hub devices as QBelt VPN servers. After setting up a VPN server in the SD-WAN cloud solution, you can add multiple VPN users, and then clients can use the QVPN Device Client to connect to the hub.

> **Note**
> You can only view the configured VPN server settings in QuRouter. To configure the settings, go to QuWAN Orchestrator.

1. Log in to QuRouter.
2. Go to **QuWAN** > **QuWAN QBelt VPN Server** .
3. Click **Go to QuWAN Orchestrator**.
   QuWAN Orchestrator opens in a new tab.
4. Log in to QuWAN Orchestrator with your QNAP ID and password.
5. Go to **VPN Server Settings** > **QuWAN QBelt VPN Server** .
6. Identify a hub.
7. Click ✎ .

> **Note**
> Hubs listed on the **QuWAN QBelt VPN Server** page are automatically configured with the default VPN server settings. You can edit the settings based on your VPN requirements.

   The VPN server configuration window appears.

8. Configure the QuWAN QBelt VPN server settings.

Setting	User Action
VPN User IP Range	Assign a fixed IP address range to the VPN users.
Subnet mask	Specify the subnet mask used to subdivide your IP address.
UDP service port	Click **Service Management** to assign a port number for the UDP service port. **Tip** Click ↻ to refresh the UDP service port number.
Maximum number of VPN users	Specify the maximum number of VPN users that can connect to the VPN server. **Note** The maximum value you can enter depends on the specified subnet mask.
DNS servers	Specify the IP address of the DNS servers. **Tip** • You can specify up to three DNS servers. • Separate entries with a comma (,).

9. Click **Save**.
   QuWAN Orchestrator saves the VPN server settings.

10. Click ○ to enable the VPN server.

The configured QuWAN QBelt VPN server settings are updated on QuRouter.

QVPN

QVPN allows you to create and manage VPN servers, add VPN clients, and monitor VPN logs.

QVPN Server Settings

QuRouter enables you to configure QNAP routers as a VPN server. You can configure multiple virtual servers to host and deliver VPN services to users in an organization.

> **Note**
> A QNAP router can support up to 30 VPN tunnels, including QuWAN and QVPN connections.

Enabling a QBelt VPN Server

QBelt is QNAP's proprietary communications protocol that incorporates Datagram Transfer Layer Security (DTLS) protocol and AES-256 encryption.

1. Log in to QuRouter.
2. Go to **QVPN Servers** > **QVPN Settings** .
3. Under QBelt, click ○ .
4. Click ⚙.
   The **QVPN Settings** window appears.
5. Configure the QBelt server settings.

Setting	Description
Client IP pool	Specify a range of IP addresses available to connected VPN clients. **Important** By default, this server reserves the use of IP addresses between 198.18.2.2 and 198.18.2.254. If another connection is configured to use this range, an IP conflict error will occur. Before adding this server, ensure a VPN client isn't configured to use this range as well.
Service Port (UDP)	Select the port used to access the server. **Note** Default port number: 4433

Setting	Description
Pre-shared key	Specify a pre-shared key (password) to verify connecting VPN clients. **Tip** Pre-shared key requirements: • Length: 8–16 ASCII characters • Valid characters: A–Z, a–z, 0–9
DNS	Specify a DNS server for the QBelt server. **Note** The DNS server limitation is 1 by default.

6. Click **Apply**.

QuRouter saves the QBelt server settings.

Enabling an L2TP VPN Server

1. Log in to QuRouter.
2. Go to **QVPN Servers** > **QVPN Settings** .
3. Under L2TP, click ◯ .

> **Important**
> You cannot enable the L2TP server if the router is using the QuWAN service.
> To enable the L2TP server, go to **QuWAN** > **QuWAN Settings** and click **Leave the organization and QuWAN**.

4. Click ⚙ .
   The **QVPN Settings** window appears.
5. Configure the L2TP server settings.

Setting	Description
Client IP pool	Specify a range of IP addresses available to connected VPN clients. **Important** By default, this server reserves the use of IP addresses between 198.18.3.2 and 198.18.3.254. If another connection is configured to use this range, an IP conflict error will occur. Before adding this server, ensure a VPN client isn't configured to use this range as well.
Authentication	Select one of the following authentication methods: • **PAP** • **MS-CHAPv2**

Setting	Description
Pre-shared key	Specify a pre-shared key (password) to verify connecting VPN clients. **Tip** Pre-shared key requirements: • Length: 8–16 ASCII characters • Valid characters: A–Z, a–z, 0–9
DNS	Specify a DNS server for the L2TP server. **Note** The DNS server limitation is 1 by default.

6. Click **Apply**.

QuRouter saves the L2TP server settings.

Enabling an OpenVPN VPN Server

1. Log in to QuRouter.
2. Go to **QVPN Servers** > **QVPN Settings** .
3. Under OpenVPN, Click ○ .
4. Click ⚙ .
   The **QVPN Settings** window appears.
5. Configure the OpenVPN server settings.

Setting	Description
Client IP pool	Specify a range of IP addresses available to connected VPN clients. **Important** By default, this server reserves the use of IP addresses between 198.18.4.2 and 198.18.4.254. If another connection is configured to use this range, an IP conflict error will occur. Before adding this server, ensure a VPN client isn't configured to use this range as well.
Service Port	Select from the following options: • **TCP** • **UDP** **Note** Default port number: 1194

Setting	Description
Encryption	Select from the following encryption methods: • **Medium (AES 128-bit)** • **High (AES 256-bit)**
DNS	Specify a DNS server for the OpenVPN server. **Note** The DNS server limitation is 1 by default.

6. Enable **Use this connection as a default gateway for remote devices**.

> **Note**
> Enable to allow the default network gateway to be redirected across the OpenVPN server. All non-local traffic from the client is transferred through the VPN server.

7. Enable **Enable compressed VPN link**.

> **Note**
> This setting compresses data before transferring it over the VPN. This will increase data transfer speeds, but requires additional CPU resources.

8. Click **Apply**.
   QuRouter saves the OpenVPN server settings.

9. Optional: Click ⤓ to download configuration files to set up an OpenVPN server manually.

Enabling a WireGuard VPN Server

1. Log in to QuRouter.

2. Go to **QVPN Servers** > **QVPN Settings** .

3. Enable WireGuard.

   a. Identify the WireGuard server.

   b. Click ⚙. The **WireGuard Settings** page appears.

   c. Click **Enable the WireGuard server**.

   d. Configure the WireGuard server settings.

Setting	User Action
Client IP pool	Enter a fixed IP subnet for the VPN server. **Important** By default, this server reserves the use of IP addresses from 198.18.7.1/24. If another connection is configured to use this range, an IP conflict error will occur. Before adding this server, ensure a VPN client is not configured to use this range as well.

Setting	User Action
Listen port	Specify a UDP port number between 1 and 65535. **Note** The default WireGuard port number is 51820.
Private key	Click **Generate Keypairs** to automatically populate a unique 32-byte private key.
DNS	Specify a DNS server for the WireGuard server.
Persistent keepalive	Specify the interval in seconds to send keepalive packets if the peer is behind a firewall.

4. Click **Apply**.
   The WireGuard settings screen closes.

5. Click ○ .
   A confirmation message appears.

6. Click **Yes**.

QuRouter enables the WireGuard server.

Adding a QVPN User

1. Log in to QuRouter.

2. Go to **QVPN Servers** > **QVPN User Management** > **QVPN User Settings** .

3. Add an L2TP, OpenVPN, or a QBelt QVPN user.

   a. Click **Add**.

   b. Specify the username and password.

> **Tip**
> Specify a password between 8 and 16 characters, containing at least one letter (A-Z, a-z) and one number (0-9).

   c. Click **Apply**.

4. Add a WireGuard QVPN user.

   a. Click **Add**.

   b. Specify a user profile name.

   c. Click **Generate Keypairs** to generate a private and public key.

   d. Click **Add**.

QuRouter adds the VPN user.

QVPN Client Settings

With the QVPN client service, you can connect the router to remote VPN servers using the OpenVPN protocol.

Important

- When adding an OpenVPN connection, an OpenVPN configuration file is required to establish the connection.
- To enable QVPN client service, ensure that you disable QVPN server service and QuWAN service.

Creating an OpenVPN Connection Profile

1. Log in to QuRouter.
2. Go to **QVPN Clients** > **QVPN Connection Profiles** .
3. Click **Add Profile**.
   The **Create an OpenVPN Connection** window appears.
4. Configure the OpenVPN connection profile.

Setting	User Action
OpenVPN connection profile	Add an OpenVPN configuration file. **a.** Click **Browse**. A File Explorer window opens. **b.** Locate the OpenVPN configuration file. **c.** Click **Open**.
OpenVPN connection profile name	Specify a name to help identify this profile.
Username	Specify the username to access the VPN server.
Password	Specify a password to access the VPN server. **Tip** Password requirements: • Length: 1–64 ASCII characters • Valid characters: A–Z, a–z, 0–9

5. Select **Automatically reconnect to OpenVPN after restarting the server**.
6. Click **Add**.

QuRouter adds the QVPN connection profile.

Enabling the QVPN Client Service

1. Log in to QuRouter.
2. Go to **QVPN Clients** > **QVPN Connection Profiles** .
3. Select an active profile.
4. Click ○ .

QuRouter enables the QVPN client service.

> **Tip**
> To view the QVPN connection logs, go to **QVPN Clients** > **QVPN Connection Logs** .

Deleting a QVPN Connection Profile

1. Log in to QuRouter.
2. Go to **QVPN Clients** > **QVPN Connection Profiles** .
3. Identify a connection profile.
4. Click 🗑.
   A confirmation message appears.
5. Click **Yes**.

QuRouter deletes the QVPN connection profile.

> **Note**
> Deleting an active QVPN connection profile automatically disables the QVPN client service.

Managing QVPN Logs

QuRouter records actions performed by QVPN servers and clients. Recorded information includes connection dates, connection duration, client names, source IP addresses, and protocol information.

1. Log in to QuRouter.

Option	UI Path
QVPN server logs	**QVPN Servers** > **Logs** .
QVPN client logs	**QVPN Clients** > **QVPN Connection Logs** .

2. To clear QVPN logs, click **Clear Logs**.
   A confirmation message appears.
3. Click **Yes**.

QuRouter clears the QVPN logs.

Service Port Management

The **Service Port Management** feature allows you to easily manage any custom network service ports on your router. You can add customized services for communication with external applications or devices.

Adding a Custom Service Port

1. Log in to QuRouter.
2. Go to **Service Port Management**.
3. Click **Add Custom Service**.
   The **Add Custom Service** window appears.

4. Specify the custom service information.

Setting	User Action
Service name	Specify a name for the service.
Protocol	Select from the following network transport protocol: • **All (TCP+UDP)** • **TCP** • **UDP** • **ESP**
WAN service port	Specify a port number. **Tip** • Ports must be between 1 - 65535 • This field can have up to 15 ports. • Separate multiple ports with commas (,) • Use hyphens (-) without a space to indicate a port range
Description	Add a description for the custom service.

5. Click **Save**.

QuRouter adds the custom service port.

Deleting a Custom Service Port

1. Log in to QuRouter.
2. Go to **Service Port Management**.
3. Identify a custom service port.
4. Click 🗑.
   A confirmation message appears.
5. Click **Yes**.

QuRouter deletes the custom service port.

DDNS Settings

Dynamic DNS Service (DDNS) allows internet access to the router using a domain name instead of an IP address. This ensures that the router is accessible even if the client ISP changes the IP assignment.

Configuring DDNS (My DDNS) Settings

1. Log in to QuRouter with your QNAP ID and password.
2. Go to **DDNS**.

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

4. Select the WAN interface.

Setting	User Action
WAN Interface	Select a configured WAN port.
Static IP	Manually assign a fixed IP address.
Obtain an Automatic DHCP IP Address	If the network supports DHCP, the adapter automatically obtains the IP address and network settings.

5. Click **Apply**.
   QuRouter updates the DDNS settings.

6. Click ○.

QuRouter enables the DDNS service.

Modifying the DDNS Domain Name

You can edit the DDNS domain name to change the address used to access the device.

1. Log in to QuRouter.

2. Go to **DDNS Settings**.

3. Click **Edit Domain Name**.
   The **Edit Device Name** window appears.

4. Enter the DDNS domain name.

> **Note**
> The myQNAPcloud domain name must be between 3 and 15 characters and can contain letters (A-Z, a-z) and numbers (0-9).

5. Click **OK**.

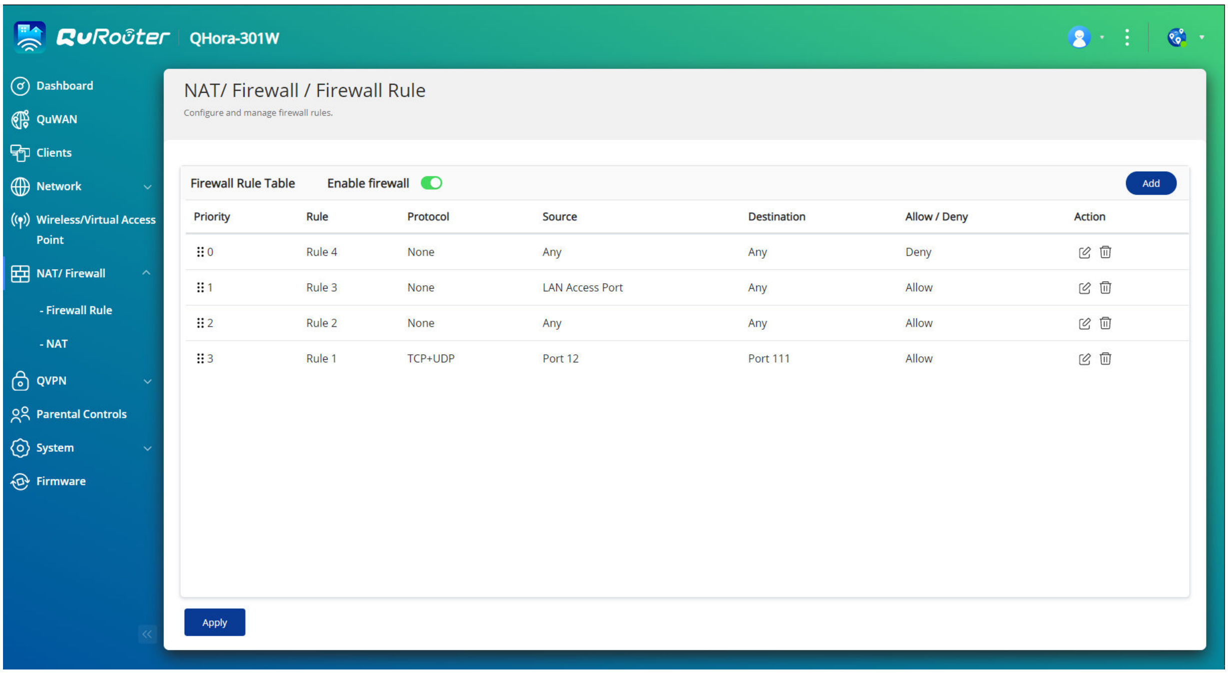
QuRouter updates the DDNS domain name.

8. Security Settings

Firewall

Firewall rules allow you to control information flow in individual packets and configure permissions according to a defined criterion.

From here you can enable the firewall and manage individual firewall rules.



NAT/ Firewall / Firewall Rule

Configure and manage firewall rules.

Firewall Rule Table   Enable firewall

Priority	Rule	Protocol	Source	Destination	Allow / Deny	Action
0	Rule 4	None	Any	Any	Deny	
1	Rule 3	None	LAN Access Port	Any	Allow	
2	Rule 2	None	Any	Any	Allow	
3	Rule 1	TCP+UDP	Port 12	Port 111	Allow	

Adding a Firewall Rule

1. Go to **NAT/Firewall** > **Firewall Rule** .
2. Click **Add**.
   The **Add Rule** window appears.
3. Configure the firewall rule settings.

Setting	User Action
Rule Name	Specify a firewall rule name. **Note** Requirements: • Length: 1–32 characters • Valid characters: A–Z, a–z, 0–9
Protocol	Specify the IP protocol type for this rule.

Setting	User Action
Source	Specify the connection source for this rule. • Selecting **Any** applies this rule to all connections. • Selecting **Define** applies this rule to traffic coming from the sources defined for this rule. • Selecting **None** allows you to apply the rule to traffic coming from the client operating system. • Selecting **Interface** allows you to apply the rule to traffic originating from all the IP addresses from the selected WAN, LAN, or VLAN interface. • Selecting **IP** allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range.
Destination	Specify the connection destination for this rule. • Selecting **Any** applies this rule to all connections. • Selecting **Define** applies this rule to traffic directed to all destinations defined for this rule. • Selecting **IP** allows you to apply the rule to connections going to a single IP, a specific subnet, or every IP within a specific range. • Selecting **Domain name** allows you to apply the rule to traffic going to all the IP address associated with the specified domain name.
Port	Specify the IP protocol type for this rule. This field is available only if you select the **TCP** or **UDP** protocol. **Note** • Ports must be between 1 - 65535 • This field can have up to 15 ports. • Separate multiple ports with commas (,) • Use hyphens (-) without a space to indicate a port range
Action	Specify whether this rule allows or blocks matching connections.

4. Click **Save**.

QuRouter creates the firewall rule.

Configuring a Firewall Rule

1. Go to **NAT/Firewall** > **Firewall Rule** .
2. Identify a role.
3. Click ✎.
   The **Edit Rule** window appears.
4. Configure the firewall rule settings.

For details, see Adding a Firewall Rule.

5. Click **Save**.

QuRouter updates the firewall rule.

Deleting a Firewall Rule

1. Go to **NAT/Firewall** > **Firewall Rule** .
2. Identify a firewall rule.
3. Click 🗑.
   A confirmation message appears.
4. Click **Apply**.

QuRouter deletes the firewall rule.

Network Address Translation (NAT)

NAT allows private networks that use unregistered IP addresses to connect to the internet. NAT translates private IP addresses in the internal network to public IP addresses before forwarding the packets onto another network.

Application Layer Gateway (ALG)

The ALG function allows you to implement transparent network translation on certain application layer protocols. NAT ALG supports the following protocols:

- File Transfer Protocol (FTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Session Initiation Protocol (SIP)

You can enable the functionality for each protocol by enabling the switch located next to the protocol name.

Port Forwarding

You can configure port forwarding rules that can be used to direct incoming and outgoing traffic on your router to a device connected to your network.

Adding a Port Forwarding Rule

Before configuring port forwarding rules, ensure you add custom service ports in **Service Port Management**. For details, see Adding a Custom Service Port.

1. Go to **NAT/Firewall** > **NAT** > **Port Forwarding** .
2. Click **Add Rule**.
   The **Add Rule** window appears.
3. Configure the rule settings.

Setting	User Action
WAN service port	Select the custom WAN service port from the drop-down menu.
WAN port	Select the WAN port from the drop-down menu.
Host IP address	Specify the LAN IP address.
LAN service port	Specify a service port number for the host IP address.
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.

4. Click **Apply**.

QuRouter adds the port forwarding rule.

Configuring a Port Forwarding Rule

1. Go to **NAT/Firewall** > **NAT** > **Port Forwarding** .
2. Identify a rule to configure.
3. Click ✎ .
   The **Edit Rule** window appears.
4. Configure port forwarding settings.
   For details, see Adding a Port Forwarding Rule.
5. Click **Apply**.

QuRouter updates the port forwarding rule.

Deleting a Port Forwarding Rule

1. Go to **NAT** > **Port Forwarding** .
2. Identify a rule.
3. Click 🗑 .
   A confirmation message appears.
4. Click **Apply**.

QuRouter deletes the rule.

Demilitarized Zone (DMZ)

A Demarcation Zone or Demilitarized Zone (DMZ) creates a publicly accessible subnetwork behind your firewall. Configuring a DMZ rule allows you to add public services to your WAN without compromising the overall security of your network.

Important

> You can configure DMZ rules only on configured WAN interfaces that are not in use by port forwarding rules.

Configuring DMZ Settings

1. Go to **NAT/Firewall** > **NAT** > **Demilitarized Zone (DMZ)**.
2. Identify a DMZ rule.

> **Note**
>
> - 1GbE WAN port 1 is used as the default interface for the DMZ rule.
> - Each configured WAN port is allowed one DMZ rule.

3. Click ⚙.
   The **DMZ Settings** window appears.
4. Specify the subnet IP address for the DMZ rule.
5. Click **Apply**.
   QuRouter applies the settings.
6. Click ○.
   QuRouter enables the DMZ rule.

Resetting a DMZ Rule

1. Go to **NAT/Firewall** > **NAT** > **Demilitarized Zone (DMZ)** .
2. Identify a DMZ rule.
3. Click **Reset**.

QuRouter resets the DMZ rule.

Discovery Settings

QuRouter enables you to locate and manage network infrastructure on your domain.

Configuring Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a networking protocol that enables dynamic port opening for peer-to-peer device communication on the network.

> **Important**
> Enabling UPnP makes the device automatically discoverable on the internet and potentially vulnerable to malware infections. Disable this feature when not in operation.

1. Go to **NAT/Firewall** > **UPnP** .
2. Click ○ .
   The device enables the UPnP function.

3. Beside WAN interface, click ⚙.
   The **Select WAN Interface** window appears.

4. Select the WAN port.

5. Click **OK**.

QuRouter applies the UPnP settings.

> **Tip**
> You can view the VLAN-enabled UPnP in **UPnP Service List**. By default, UPnP is enabled on VLAN 1 and the device advertises itself to plug and play devices connected to VLAN 1.

Parental Controls

QuRouter provides parental control functions to manage content filtering, safe search, and protect connected clients from inappropriate and harmful content. Network administrators can create custom parental control rules to limit internet access, block websites, and assign rules to connected devices.

Adding a Parental Control Role

1. Go to **Parental Controls**.

2. Click **Add Role**.
   The **Add Role** window appears.

3. Configure the role settings.

Setting	User Action
Role name	Specify a name for the parental control role.
Enable website filter	Select this option to enable website filtering to prevent users from viewing certain URLs or websites.
Domain Name Filter	Enter an entire domain name or specific URLs. Separate multiple URLs with commas (,).
Safe Search	Enable safe search to filter out explicit content in the following sites: • **YouTube** **Note** You can select from the following restriction modes: • **Restricted**: Completely block potentially mature and violent content. • **Medium**: Partially allow explicit and adult-oriented content. • **Google** • **Bing**

4. Click **Apply**.

QuRouter creates the parental control role.

Configuring a Parental Control Role

1. Go to **Parental Controls**.
2. Identify a role.
3. Click ✎.
   The **Edit Role** window appears.
4. Configure the parental role settings.
   For details, see Adding a Parental Control Role.
5. Click **Apply**.

QuRouter updates the parental control role.

Deleting a Parental Control Role

1. Go to **Parental Controls**.
2. Identify a role.
3. Click 🗑.
   A confirmation message appears.
4. Click **Apply**.

QuRouter deletes the role.

Adding a Device to a Parental Control Role

> **Note**
> You cannot assign a single device to more than one role at a time.

1. Go to **Parental Controls**.
2. Identify a role to add to a device.
3. Click **Add Device**.
   The **Add Device** window appears.
4. Select a wireless device from the list.
5. Click **Add**.

QuRouter adds the device to the parental control role.

Deleting a Device from a Parental Control Role

1. Go to **Parental Controls**.
2. Identify the device to delete.
3. Click 🗑.

A confirmation message appears.

4. Click **OK**.

QuRouter removes the device from the parental control role.

Quality of Service (QoS)

Quality of service (QoS) improves network traffic shaping by classifying and prioritizing different network devices and packets. QoS allows you to configure traffic policies and enabling these policies on the switch ports.

To configure QoS settings, you must add the device to the QuWAN service and configure the settings using QuWAN Orchestrator.

Configuring QoS Settings on QuWAN Orchestrator

1. Log in to QuRouter.
2. Go to **QuWAN** > **Quality of Service (QoS)** .
3. Click **QoS Configuration on QuWAN Orchestrator**.
4. Log in to QuWAN Orchestrator.
5. Go to **QuWAN Device**.
6. Select the region and your device.
7. Click **Quality of Service**.
8. Under **Quality of Service**, click **Add**.
   The **Add Quality of Service Rule** window appears.
9. Specify a rule name.
10. Configure rule settings.

Setting	User Action
Source	Specify the connection source for the rule. • Selecting **Any** applies this rule to all connections. • Selecting **Define** applies this rule to traffic coming from the sources defined for this rule. • Selecting **None** allows you to apply the rule to traffic coming from the client operating system. Specify the client OS from the drop-down list. • Selecting **IP** allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range.

Setting	User Action
Destination	Specify the connection destination for this rule. • Selecting **Any** applies this rule to all connections. • Selecting **Define** applies this rule to traffic directed to all destinations defined for this rule. • Selecting **None** allows you to apply the rule to traffic going to the client operating system. Specify the client OS from the drop-down list. • Selecting **IP** allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range. • Selecting **Domain name** applies the rule to a specific domain name.
Protocol	Specify the network transport protocol for the rule.
Port	Specify the service port number. This field is only available if the TCP or UDP protocol is selected. **Tip** • Specify a port number between 1 and 65535. • Enter up to 15 ports. • Separate multiple ports with commas (,). • Use hyphens (-) without spaces to indicate a port range.
Application	Specify whether this rule allows or blocks specific applications or application categories. • Selecting **Any** applies this rule to all applications and application categories. • Selecting **Define** applies this rule to traffic directed to all applications and categories defined for this rule.
Action	• Service class: Specify the service class priority from the drop-down list. • Network steering: Select the band steering method to steer traffic based on the QoS markings on the packets. • **Auto**: QuWAN Orchestrator automatically detects the optimal transmission path for steering traffic. • **Direct**: Manually select the WAN port to steer traffic.

11. Click **Create**.

QuWAN Orchestrator adds the QoS rule.

9. Troubleshooting

This chapter describes basic troubleshooting information.

Support and Other Resources

QNAP provides the following resources:

Resource	URL
Documentation	https://docs.qnap.com
Service Portal	https://service.qnap.com
Downloads	https://download.qnap.com
Community Forum	https://forum.qnap.com

Testing Network Connectivity with the Ping Utility

Ping uses Internet Control Message Protocol (ICMP) query messages, ICMP echo messages, and ICMP echo replies to verify device connectivity.

1. Log in to QuRouter.
2. Go to **System** > **Diagnostics** .
3. Configure the ping utility settings.
4. Select **Ping IPv4** as the diagnostic utility.
5. Select the WAN interface from the drop-down menu.
6. Specify an IP address or domain name.
7. Specify the number of echo requests to be sent and received.

   Note
   Specify a number between 1 and 50.

8. Click **Ping IPv4**.

QuRouter generates the data for the specified diagnostic utility.

Tip
To clear the generated data from QuRouter, click **Clear**.

Testing Network Connectivity with the Traceroute Utility

Traceroute discovers which route a packet travels between a source and destination. Traceroute records each ICMP time exceeded message and generates a trace of the path the packet took to reach the destination.

1. Log in to QuRouter.
2. Go to **System** > **Diagnostics** .
3. Configure the traceroute utility settings.

4. Select **Traceroute** as the diagnostic utility.
5. Select the WAN interface from the drop-down menu.
6. Specify an IP address or domain name.
7. Click **Traceroute**.

QuRouter generates the data for the specified diagnostic utility.

> **Tip**
> To clear the generated data from QuRouter, click **Clear**.

Using QNAP Remote Support to Resolve Router Issues

Remote Support allows the QNAP Customer Service team to access and assist you with router-related issues.

1. Log in to QuRouter.
2. Click ⋮.
3. Click **QNAP Remote Support**.
   The **QNAP Remote Support** window opens.
4. Create a support ticket.
   a. Click **Create a support ticket**.
      The QNAP Customer Service site opens in your browser.
   b. Click **sign in**.
   c. Log in with your QNAP ID and password.
   d. Click **Support**.
   e. Click **Create Support Ticket**.
      The **Create Support Ticket** page appears.
   f. Configure the ticket settings.

Setting	User Action
Device serial number	Select a registered product serial number from the drop-down menu. **Tip** You can also enter a device serial number that is not registered with your QNAP ID.
Model	Enter the model number of the device. **Note** The model number is automatically populated when selecting the device serial number is entered.
Firmware	Enter the firmware build number.
Client device	Select the client device operating system from the drop-down menu.

Setting	User Action
Issue category	Select from the following: • **Hardware Failure** • **Software Issue**
Device type	Select **Switch/Router** from the drop-down menu.
Issue	Select an issue category.
Subject	Specify a subject title describing the issue.
Description	Describe the router issue in between 0 and 1000 characters. **Tip** • You can upload images or log files up to 35 MB. • To download diagnostic logs, go to **System** > **Event logs** , and then click **Export**.

g. Confirm your contact information.

h. Click **Send Message**.
QNAP Customer Service sends an email to your QNAP ID that includes a support ticket ID.

5. Allow remote connections from the Customer Service team.

a. Log in to QuRouter.

b. Click ⋮.

c. Click **QNAP Remote Support**.
The **QNAP Remote Support** window opens.

d. Enter the support ticket ID and your QNAP ID.

e. Click **Next**.
The **Terms of Service** window appears.

f. Read and accept the terms of service.

g. Click **Next**.
QuRouter creates a temporary account, password, and private key for the QNAP Customer Service team.

h. Click **Confirm**.

QNAP Customer Service team establishes a remote connection to your router.

10. Glossary

myQNAPcloud

Provides various remote access services such as DDNS and myQNAPcloud Link

QNAP ID

User account that enables you to use myQNAPcloud remote access and other QNAP services

Qfinder Pro

QNAP utility that lets you locate and access QNAP devices in your local area network

QuRouter

The QNAP web management interface that allows you to view and configure QNAP routers

QuWAN

QNAP SD-WAN management system

QuWAN Orchestrator

QNAP centralized management cloud platform for SD-WAN infrastructure

11. Notices

This chapter provides information about warranty, disclaimers, licensing, and federal regulations.

Limited Warranty

QNAP offers limited warranty service on our products. Your QNAP-branded hardware product is warranted against defects in materials and workmanship for a period of one (1) year or more from the date printed on the invoice. ("Warranty Period"). Please review your statutory rights at www.qnap.com/warranty, which may be amended from time to time by QNAP in its discretion.

Disclaimer

Information in this document is provided in connection with products of QNAP Systems, Inc. (the "QNAP"). No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in QNAP's terms and conditions of sale for such products, QNAP assumes no liability whatsoever, and QNAP disclaims any express or implied warranty, relating to sale and/or use of QNAP products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

QNAP products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

In no event shall QNAP’s liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Back up the system periodically to avoid any potential data loss is recommended. QNAP disclaims any responsibility of all sorts of data loss or recovery.

Should you return any components of the package of QNAP products for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.

All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.

Further, the ® or ™ symbols are not used in the text.

CE Notice

This QNAP device complies with CE Compliance Class B.

FCC Notice

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

> **Note**
> This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
>
> - Reorient or relocate the receiving antenna.
> - Increase the separation between the equipment and receiver.
> - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
> - Consult the dealer or an experienced radio/television technician for help.

> **Important**
> Any modifications made to this device that are not approved by QNAP Systems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

Radio Equipment Directive (RED) 2014/53/EU Article 10

RED 2014/53/EU requires that for products which could potentially have an issue with a non-harmonized frequency in a specific EU country, the product documentation must list the restrictions, and the packaging must carry a label reflecting that country's code.

This QNAP router complies with RED 2014/53/EU article 10.

EU RoHS Statement

This equipment complies with the European Union RoHS Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment. The directive applies to the use of lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls (PBB), and polybrominated diphenyl ethers (PBDE) in electrical and electronic equipment.

ISED Compliance Statement

Industry Canada has been renamed Innovation, Science, and Economic Development Canada (ISED) following the issue of RSP-100 Issue 11 and DC-01 Issue 06. Equipment certifications previously issued by Industry Canada remain valid and do not require updating. Meaning you may see the names used interchangeably in documentation. The following statement is applicable to ASiR-pRRH which has Innovation, Science and Economic Development (ISED) approval: This device complies with ICES-003 of Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Radiation Exposure Statement

This product complies with the IC radiation exposure limits set for an uncontrolled environment. To comply with RSS 102 RF exposure compliance requirements, a separation distance of at least 27 cm must be maintained between the antenna of this device and all persons. The device for the band 5150-5350 MHz is only for indoor usage to reduce potential harmful interference to co-channel mobile satellite systems.

UKCA Notice

This device complies with the UKCA requirements for products sold in Great Britain.