QHora-301W

User Guide

Contents

8. Security

9. Support and Other Resources

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 Ethernet ports	• 2 x 10 GbE RJ45 • 4 x 1 GbE RJ45
Antenna	8 x 5dBi internal antennas
Total power consumption	418W
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)	160 × 528 × 403 mm (62.99 x 207.87 x 158.66 in)

Component	QHora-301W
Net weight	4.41 kg (9.72 lbs)
Other	
Fans	Fanless
Operating temperature	0˚C to 40˚C (32˚F to 104˚F)
Relative humidity	Non-condensing relative humidity: 10% to 90%
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 802.3Q virtual LAN (VLAN)
	
	• IPv4 address routing management

Security	• Protocol-based firewall (TCP, UDP, ICMP, TCP+UDP) • IP address-based firewall rule configuration • Network Address Management (NAT) and port forwarding
VPN	• Remote access support using L2TP, OpenVPN, and QBelt (QNAP proprietary VPN) protocols • Client IP pool management • VPN client management • Connection logs • Maximum VPN tunnels: 30
Access Control	• Parental control • Domain Name Filtering (DNS) and content filtering

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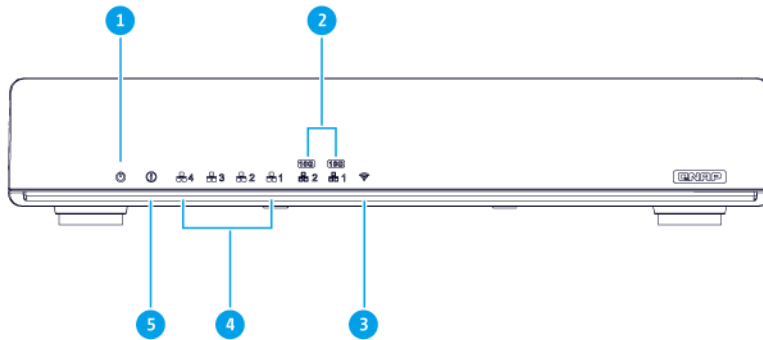
No.	Component	No.	Component
1	Power LED	4	Gigabit Ethernet activity LEDs
2	10 Gigabit Ethernet Activity LEDs	5	Router status
3	Wireless LED	-	-

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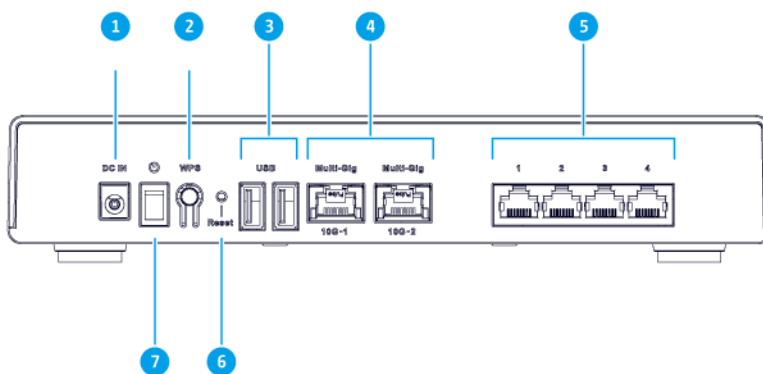
No.	Component	No.	Component
1	Power input	5	Gigabit Ethernet ports (RJ45)
2	WPS button	6	Reset button
3	USB 3.2 Gen 1 Type-A ports	7	Power switch
4	10 Gigabit Ethernet ports (RJ45)	-	-

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

Operation	User Action	Result
Reset	Press and hold the button for 3 seconds.	The router resets and all default settings are restored. The router is unbound from 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: 10% to 90% • 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 QHora with 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.

    d. Connect the router to the computer.

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

f. Connect the Ethernet cable to a Gigabit Ethernet port on the computer.
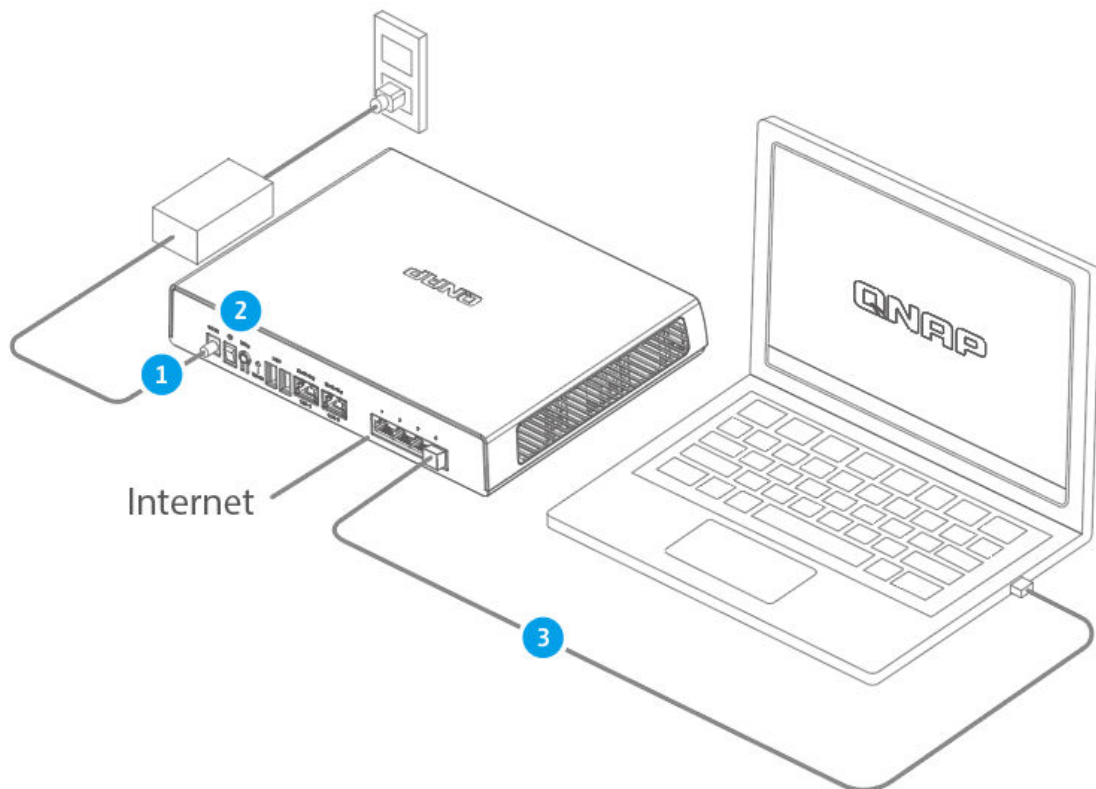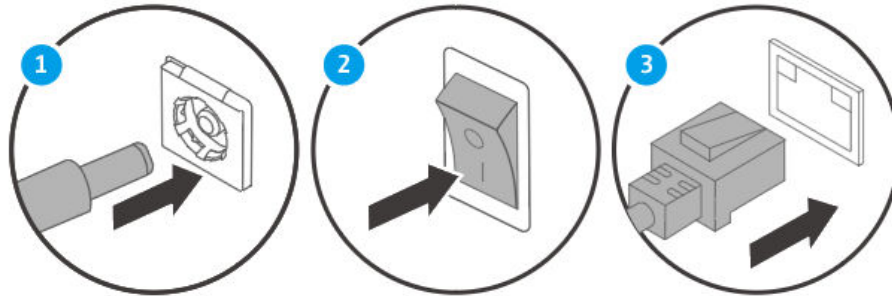
4. Verify that the router is recognized by the computer.

    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.

5. Open a web browser.

6. Enter https://192.168.100.1 to access the QuRouter web interface.

7. 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 • Logon credentials of a valid user account For details, see Accessing the Router Using a Browser.	• Computer that is 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.	• Computer that is 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 its IP address and the logon credentials of a valid user account.

> **Note**
> If you do not know the IP address of the router, you can locate it using Qfinder Pro.

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.

4. Specify the default username and password.

Default Username	Default Password
admin	The MAC address of the router image omitting any colons (:) and capitalizing any letters. 💡 **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 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/en/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	The MAC address of the router image omitting any colons (:) and capitalizing any letters. 💡 **Tip** For example, if the MAC address is 00:0a:0b:0c:00:01, the default password is 000A0B0C0001.

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

4. QuRouter

About QuRouter

QuRouter is a centralized management tool for your QNAP router. With its intuitive interface, QuRouter makes it easy to set-up, secure, and configure the features of your router.

System Requirements

Category	Detail
Hardware	QHora router

Software	• Web browser:
	
	    • Microsoft Internet Explorer 11 or later
	
	    • 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 QHora with QNAP ID.

2. Configure network settings.
   For details, see Configuring Port Definitions.

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

   • Configuring VAP Settings

   • Configuring the Guest Wireless Network

   • Configuring Wi-Fi Protected Setup (WPS)

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

   • Configuring Device Name Settings

   • Configuring Access Control Settings

   • Restart, Reset, Backup, and Restore

   • Configuring Audio Alert Settings

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

   • Adding a VPN Client

- Enabling QBelt VPN Server

- Enabling L2TP VPN Server

- Enabling 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. Alternatively, use Qfinder Pro to locate the router on the list.

3. Double-click on the name or IP address.
   The web browser opens the QuRouter web page.

4. Enter https://192.168.100.1 in the address bar to access the QuRouter web interface.

5. Click **Start**.
   The **Set Up and Access QuWAN** page appears.

6. Click **OK**.

7. Select one of the following WAN interface settings:

Setting	Description
DHCP	Obtain IP address settings automatically via DHCP
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 this option to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

8. Click **Apply**.

9. Specify the current location of the device.

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

   b. Click **Next**.
      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:

      • Works only on 2.4 GHz band consisting of channels 1 to 11

      • 5 GHz band is unavailable

      • 2.4 GHz band operates on low output power

    c. Click **OK**.

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

11. Click **Next**.

12. Specify the default username and password.

Default Username	Default Password
admin	The MAC address of the router image omitting any colons (:) and capitalizing any letters. **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 at the bottom of the device.

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

14. Optional: You can log on to QuRouter using your QNAP ID and password.
For details, see Binding QHora with QNAP ID.

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

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

17. Click **OK**.
The **Wireless Regulatory Domain Settings** page appears.

> **Note**
> QNAP regulates the wireless domain settings based on the geoIP address of the router. During the initial configuration process you must select the current location of the device and a comparison is made between the selected location and the geoIP address of the device. This ensures that the device meets the wireless regulatory domain specifications and the router can access the wireless features without any limitations.

18. Select the current device location.

    a. Click **OK**.

    b. If the system detects a mismatch between the selected location and the IP geolocation more than three times, contact QNAP Customer Service to obtain the wireless activation code and apply the settings to rectify the router regulatory domain settings.

QuRoutersaves the settings.

Enabling the Full Wireless Functionality in QuRouter

1. Open QuRouter.

2. Click **Basic Wireless Mode**.
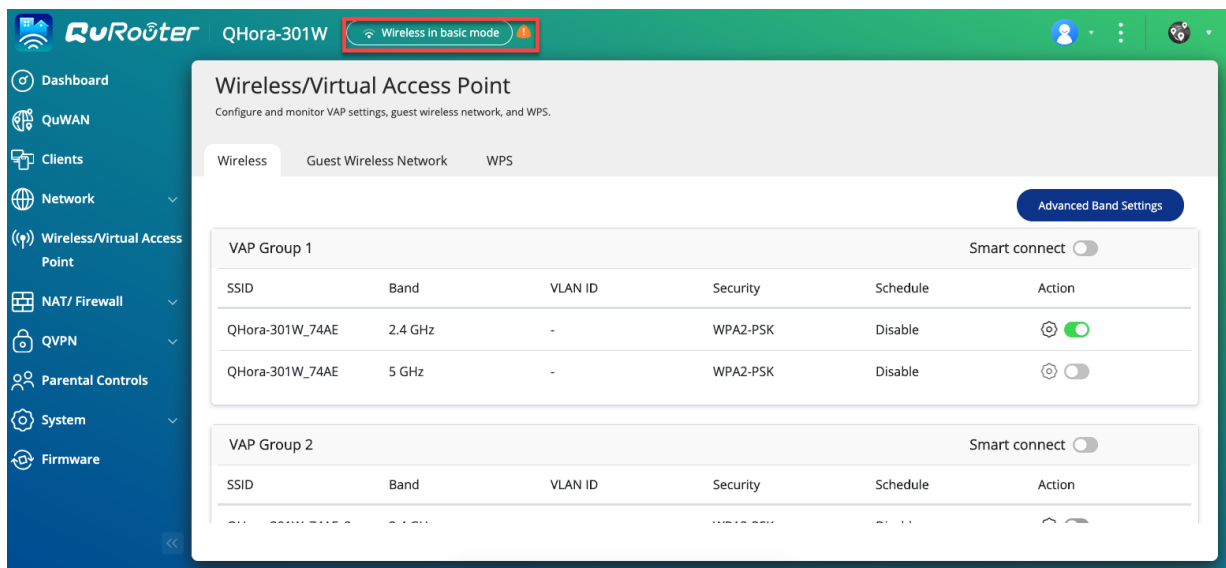
The **Wireless Regulatory Domain Settings** page appears.

3. Select the current location of the device.

4. Click **OK**.

QuRouter enables all the wireless functions of the router.

Binding the Router with QNAP ID

1. Go to QuRouter.

2. Log in with your QNAP ID and password.

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

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

4. Enter the local account credentials in order to complete the 2-step verification process.

5. Click **OK**.
   The QuRouter dashboard opens and the **Edit Device Name** window appears.

6. Specify a device name containing between 3 to 15 alphanumeric characters.

7. Click **OK**.

The router is bound to the QNAP ID.

Unbinding the Router from QNAP ID

1. Go to **System** > **Access Control** > **Administrator** .

2.
   Below **Unbind QNAP ID**, click .
   A confirmation message appears.

3. Click **OK**.

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

5. QuRouter Navigation

Task Bar

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 • **About**: Displays the following information: • Operating system • Hardware model • Firmware version
3	QuWAN	Click the button to view QuWAN-related information. • QuWAN Orchestrator connection status • Organization • QuWAN settings • Go to QuWAN Orchestrator

Dashboard
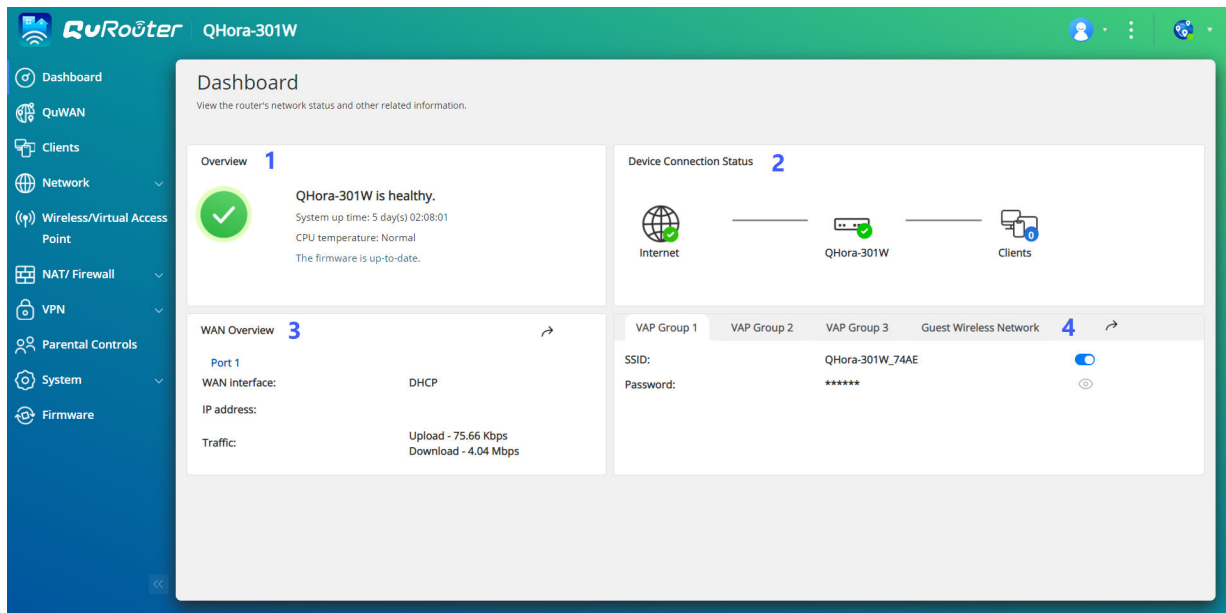
No.	Section	Displayed Information	User Action
1	Overview	• Uptime (number of days, hours, minutes and seconds) • CPU temperature • Firmware information	-
2	Device Connection Status	• Internet status • Device status • Number of connected clients	-
3	WAN Overview	• WAN interface • IP address • Traffic	Click ↗ to open **Network > WAN** .
4	Wireless/ Virtual Access Point (VAP)	VAP Groups/ Guest Wireless Network • SSID • Password	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

This sections controls the router operation modes and provides access to the following modes:

- **Wireless Router**

- **Access Point (AP)**
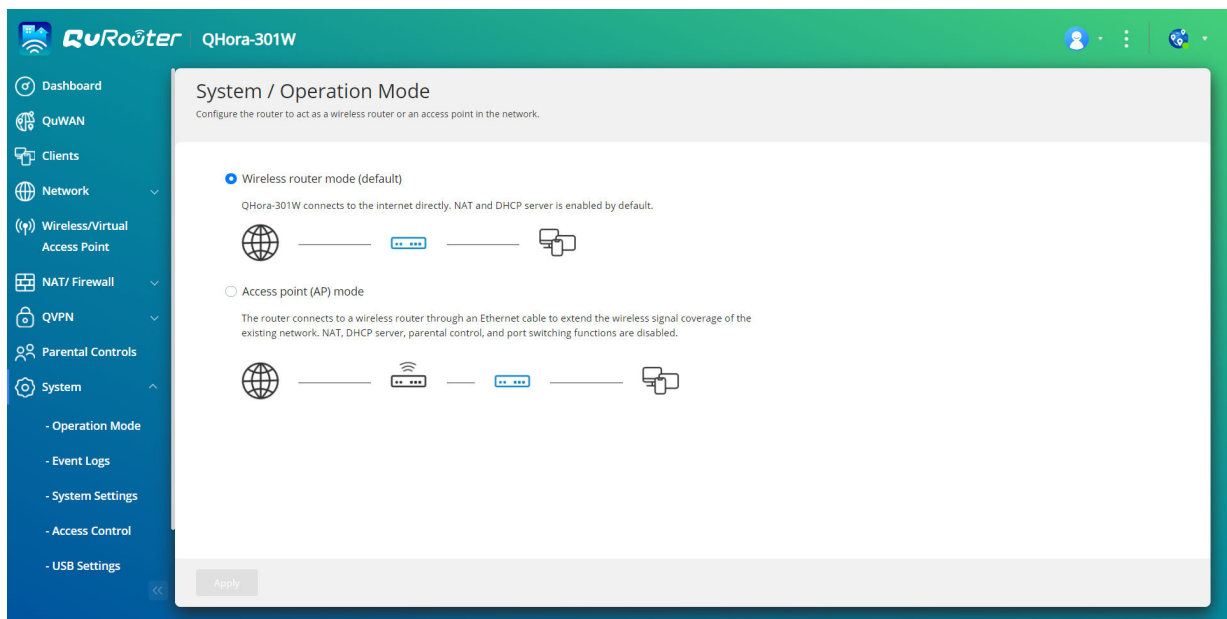
1. Go to **System** > **Operation Mode** .

2. Select from the following router operation modes:

Setting	User Action
Wireless Router Mode	This is the default router operation mode. The device acts as the wireless router in the network. **Note** The router uses NAT and DHCP server functions by default.
Access Point (AP) Mode	The device acts as the access point in the network. **Note** DHCP server, NAT, QuWAN, and WAN functions are disabled when the router operates as an access point. For details on configuring access point mode, see Configuring Access Point (AP) Mode.

3. Click **Apply**.

QuRouter applies the operation mode settings.

Configuring Access Point (AP) Mode

1. Go to **System** > **Operation Mode** .

2. Select **Access point (AP) mode**.

   a. Optional: Select **Enable Spanning Tree Protocol (STP)**.

   b. Select one of the following:

      • **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.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
DNS Server	Specify a DNS server for the DHCP server.

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

4. Click **OK**.

   ⛔ **Important**
   The following settings are changed when the router is switched to AP mode.

      • The router is unbound from QNAP ID.

      • The router is removed from the QNAP organization and QuWAN. You must reconfigure the QuWAN settings when you enable router mode.

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

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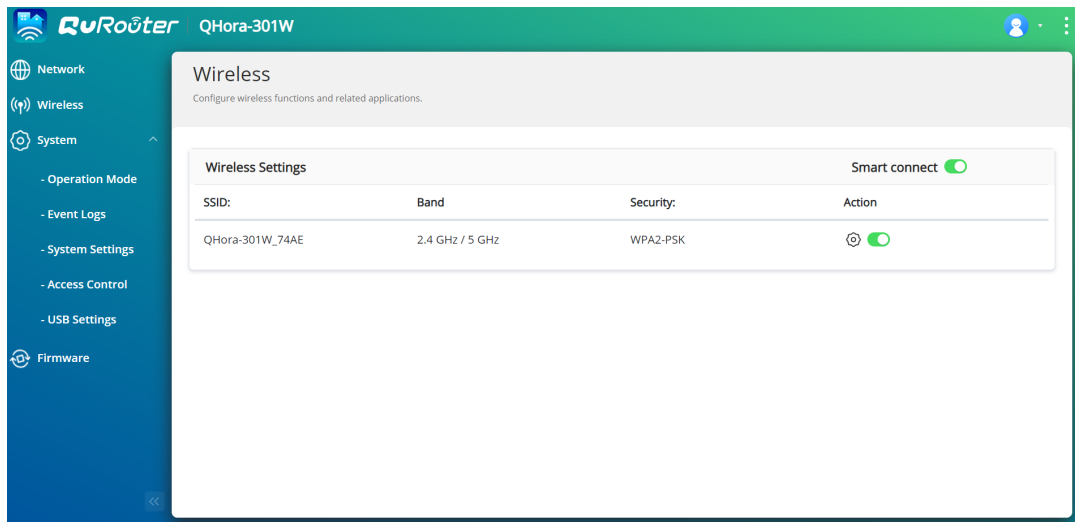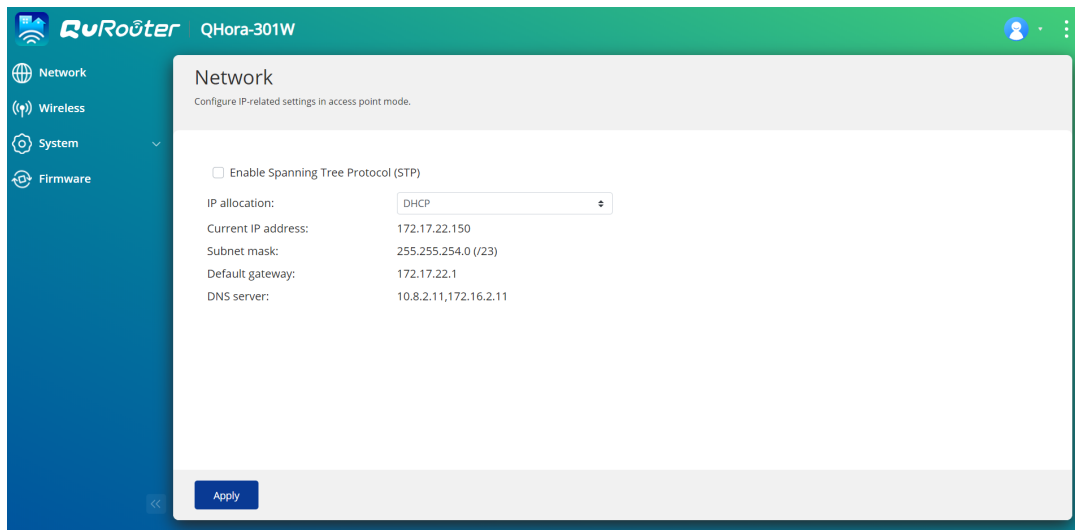   To download Qfinder Pro, go to https://www.qnap.com/utilities.

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

7. Enter the local account credentials of the router.

8. Click **Login**.

Note

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

Event Logs

This screen displays a record of events related to QuRouter. Common events include enabling or disabling network services, configuring account and system settings, and configuring security settings.
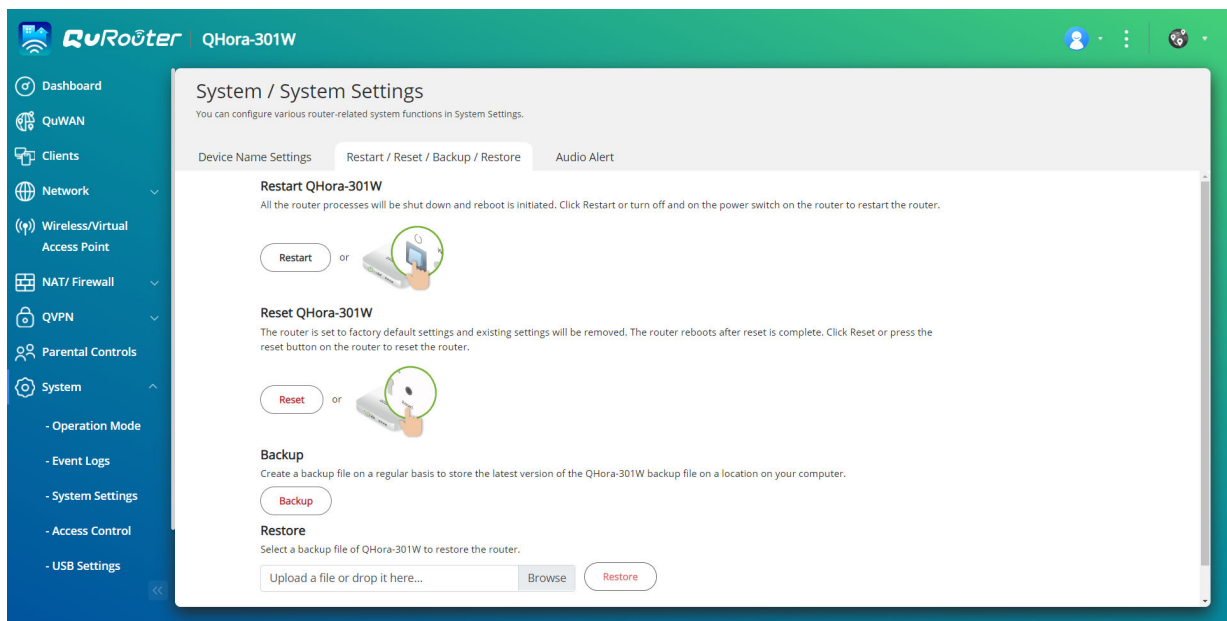
System Settings

Configuring Device Name Settings

1. Go to **System** > **System Settings** > **Device Name Settings** .

2. Click [edit icon] .
   The **Edit Device Name** window appears.

3. Specify device name that consists of 3 to 15 characters from any of the following group:
   Valid characters: A–Z, a–z, 0–9

4. Click **OK**.

QuRouter updates the device name.

Restart, Reset, Backup, and Restore

This section 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** .

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** .

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** > **Restart / Reset** .

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** > **Restart / Reset** .

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.

Configuring Audio Alert Settings

1. Go to **System** > **System Settings** > **Audio Alert** .

2.
   Click   .
   QuRouter enables audio alerts on the router.

Configuring Access Control Settings

Access Control is a security feature that enforces security policies on devices that can access the router network to increase network security and reduce security threats.

1. Go to **System** > **Access Control** > **Access Control Settings** .

2. Enable one of the following options:

Setting	Description
Local Management via HTTP	You can connect devices to internal websites via the Hypertext Transfer Protocol (HTTP). HTTP connections are faster than Hypertext Transfer Protocol Secure (HTTPS).
Remote Management	Enable this option to allow administrators remote access to the web interface of the router. **Note** Remote management cannot be disabled if you are managing the router using a WAN IP address.

Configuring Local Account Settings

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

1. Go to **System** > **Access Control** > **Administrator** .

2.
   Click   to configure local account credentials.
   The **Local Account** window appears.

3. Configure the local account settings.

Description	User Action
Username	Specify a username that contains 5 to 32 characters from any of the following groups: 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.

4. Click **OK**.

QuRouter updates the local account settings.

USB Settings

This sections allows you to access and manage USB-related settings, FTP access, and FTP users.
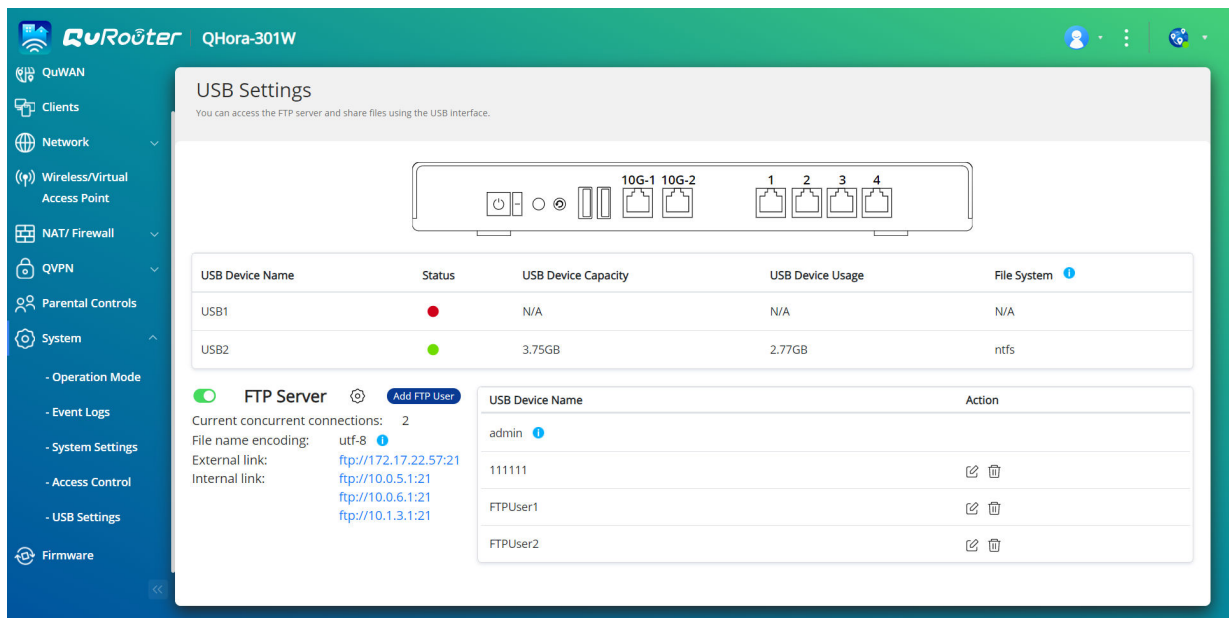
Configuring FTP Access

1. Go to **System** > **USB Settings** .

2. Enable **FTP Server**.

3.
   Click ⚙ .
   The **FTP Settings** window appears.

4. 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**

5. 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 accessing the network through the WAN segment.
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 segment.

Adding an FTP User

1. Go to **System** > **USB Settings** .

2. Click **Add FTP User**.
   The **Add FTP User** window appears.

3. Configure the FTP user settings.

Setting	User Action
Username	Enter a username that contains 5 to 32 characters from the following groups: 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.

4. Click **Add**.

QuRouter saves the FTP user information.

Configuring an FTP User

1. Go to **System** > **USB Settings** .

2. Identify an FTP user to configure.

3.
Click ✐ .
The **Edit FTP User** window appears.

4. Configure FTP user settings.
For details, see Adding an FTP User.

5. Click **Edit**.

QuRouter updates the FTP user information.

Deleting an FTP User

1. Go to **System** > **USB Settings** .

2. Identify an FTP user you want to delete.

3.
Click 🗑 .
A confirmation message appears.

4. Click **OK**.

QuRouter deletes the FTP user.

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**.

Updating the Firmware Manually

The update may require several minutes or longer, depending on your hardware configuration and network connection. Do not power off the device during the update.

1. Download the device firmware.

2. Go to http://www.qnap.com/download.

   a. Select your device model.

    b. Read the release notes and confirm the following:

        • The device 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 image file.

3. Go to **Firmware**.

4. Select **Manual update**.

5. Click **Browse** and then select the extracted firmware image file.

6. Click **Apply**.

7. Network Settings

Network

Configuring Port Definitions

1. Go to **Network** > **Port Definition** .

2. Select the WAN port configuration from the following options based on your network requirements.

Setting	Description
WAN 1 GbE port 1	Select this option 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 this option 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 this option 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.

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

4. Click **OK**.

QuRouter updates the port definition settings.

Configuring Wide Area Network (WAN) Interface Settings

1. Go to **Network** > **Port Definition** .

2. Identify the WAN interface you want to configure.

3.
   Click .
   The port configuration window appears.

4. Configure the port settings.

5. 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 this option to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

6. Specify a port description.

7. Specify an MTU value between 98 and 9000.

8. Click **OK**.

QuRouter updates the WAN settings.

Configuring Local Area Network (LAN) Access and Trunk Modes

1. Go to **Network** > **Port Definition** .

2. Identify a LAN port to configure.

3.
   Click ⚙ .
   The port configuration window appears.

4. 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 configure trunk mode. 💡 **Tip** To create a new VLAN, see Adding a VLAN.
Description	Enter a description for the port.

5. Click **OK**.

QuRouter updates the mode settings.

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. Open QuRouter.

2. Go to **Network** > **VLAN** .

3. Click **Add VLAN**.
   The **Add VLAN** window opens.

4. Specify a VLAN ID.

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

6. Specify a fixed IP address.

7. Specify the subnet mask.

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

9. 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	Click **Add** to configure a reserved IP table. Specify the following: • Device name • IP address • MAC address

10. Click **Apply**.

QuRouter adds the VLAN.

Configuring a VLAN

1. Open QuRouter.

2. Go to **Network** > **VLAN** .

3. Identify the VLAN to configure.

4.

Click ⚙ .

The **VLAN Configuration** window opens.

5. Edit the VLAN settings.

6. Click **Apply**.

QuRouter updates the VLAN.

Deleting a VLAN

1. Open QuRouter.

2. Go to **Network** > **VLAN** .

3. Identify the VLAN.

4.

Click 🗑 .

> **Note**
> You cannot delete the VLAN if it being utilized by a WAN or LAN port.
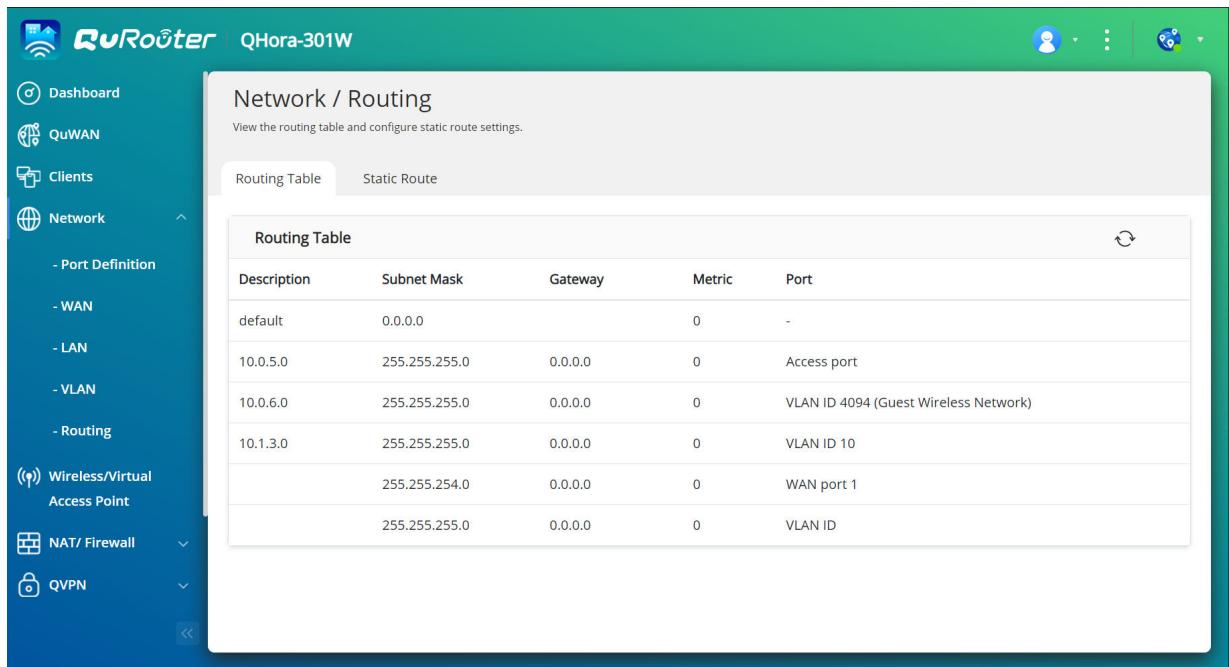
A confirmation message appears.

5. Click **Delete**.

QuRouter deletes the VLAN.

Routing Table

This section lists routing table entries from the following sources:

- directly connected networks

- dynamic routing protocols

- statically configured routes

Static Route

This section controls the creation of static routes. 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.

Adding a Static Route

1. Go to **Network** > **Routing** > **Static Route** .

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

3. 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 netmask.
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.

4. Click **Apply**.

QuRouter creates the static route.

Configuring a Static Route

1. Go to **Network** > **Routing** > **Static Route** .

2. Identify a route.

3. Click ✎ .
The **Edit Static Route** window appears.

4. Configure the static route settings.
For details, see Adding a Static Route.

5. Click **Apply**.

QuRouter updates the static route settings.

Deleting a Static Route

1. Go to **Network** > **Routing** > **Static Route** .

2. Identify a route.

3. Click 🗑 .
A confirmation message appears.

4. Click **Apply**.

QuRouter deletes the route.

Wireless/Virtual Access Points

Virtual Access Point (VAP)

You can configure multiple virtual access groups from a single physical access point using VAP. Each VAP group can be configured with its own security features that can be used to control access to wireless devices and implement security protocols. This section controls VAP group settings, including Smart Connect, wireless scheduler, and security protocols.
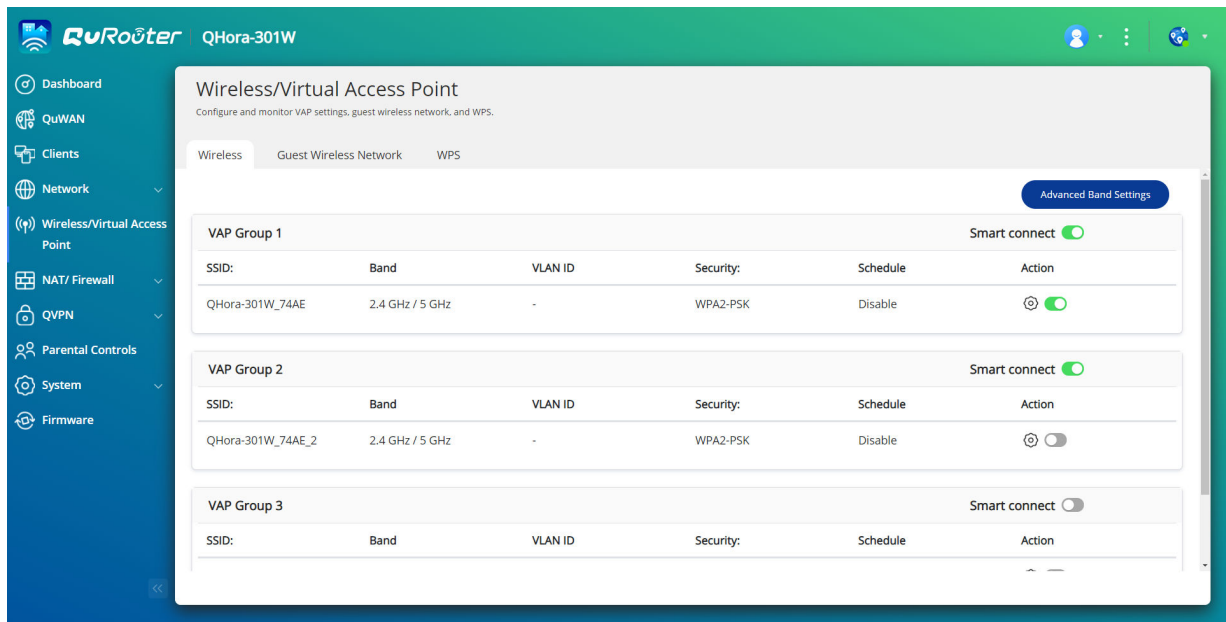
Configuring VAP Settings

1. Go to **Wireless/Virtual Access Point** > **Wireless** .

2. Identify a VAP group you want to configure.

3. Optional: Enable **Smart Connect** if you want the VAP group to operate 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 VAP 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.

Setting	User Action
SSID	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.
Security	Select a security authentication method from the following options:
Password	Enter a password that contains 8 to 63 characters. **Note** The password is case-sensitive.
Enable 802.11r Fast Roaming	Select this option 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 VAP group.

6. Click **Apply**.

QuRouter updates the VAP group settings.

Configuring Advanced Band Settings on VAP 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 this option 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.

Setting	User Action

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**

Enable DFS Channels	Enable Dynamic Frequency Selection (DFS) to utilize more channels and avoid wireless interference.
Channels	Select the DFS channel that is less frequently used. **Note** The channel is set to **Auto** by default to avoid radio frequency interference.
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.

Setting	User Action
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.
Password	Specify a password that contains 8 to 63 characters. **Note** The password is case-sensitive.

4. Click **Apply**.

QuRouter saves the guest wireless network settings.

Wi-Fi Protected Setup (WPS)

The WPS protocol is a standard that allows you to easily configure a wireless network without the additional requirement of configuring wireless network names (SSID) and security specifications.
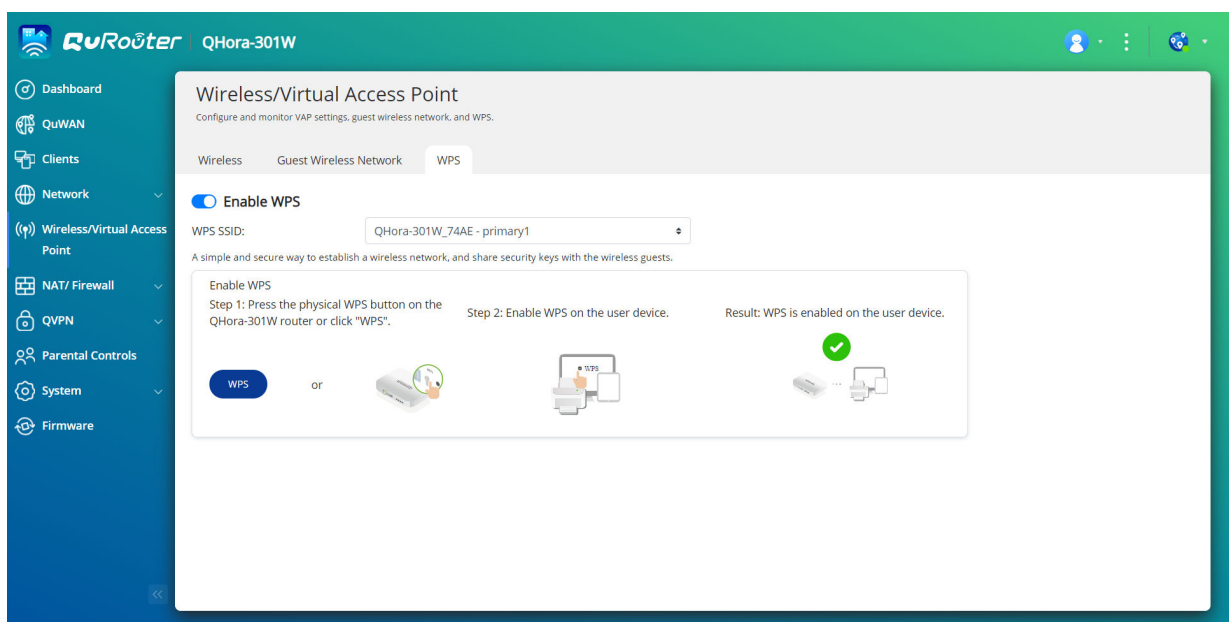
Configuring Wi-Fi Protected Setup (WPS)

1. Go to **Wireless/ Virtual Access Point** > **WPS** .

2.
   Click ⬤ .
   The WPS function is enabled.

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 allows you to access wired and wireless clients connected to the router network. You can also add clients to or remove clients from the blocked list.

Client List

The Client List displays the list of wired and wireless devices connected to the router. You can also add a device to or remove a device from the blocked list.

Blocked List

This screen controls the management of clients blocked from accessing wired and wireless services.
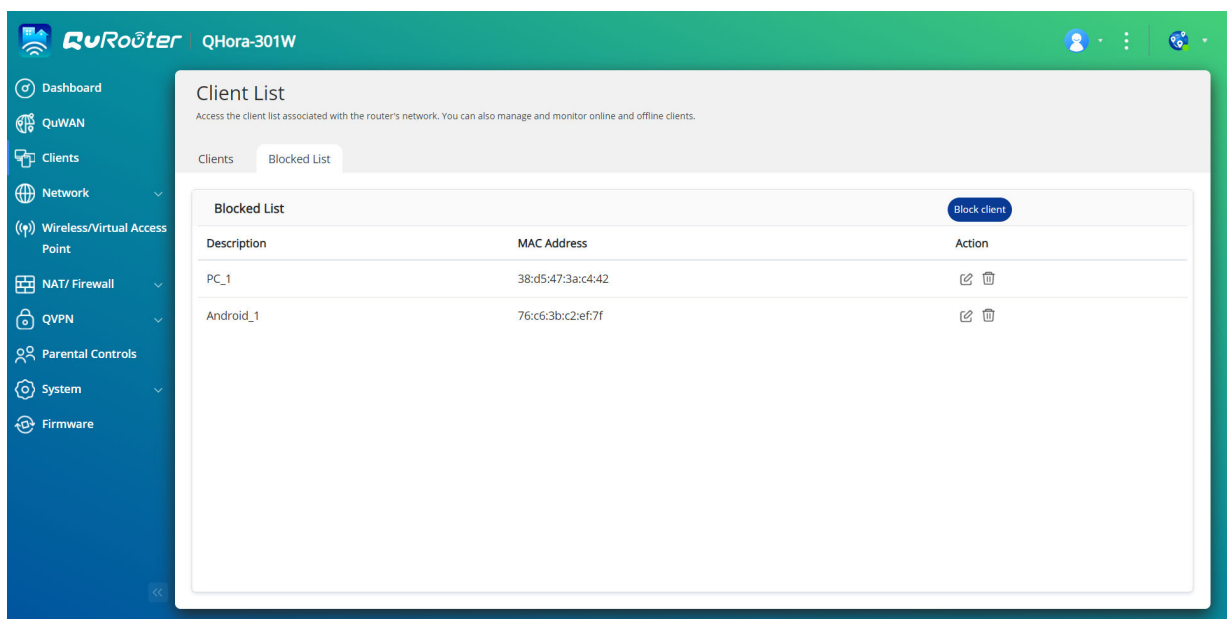
Adding a Device to Blocked List

1. Go to **Clients** > **Blocked List** .

2. Click **Block Client**.
   The **Add Device to Blocked List** window appears.

3. Configure the blocked list settings.

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

Tip
You can restrict the device from accessing any or all networks by selecting the Virtual Access Point (VAP) groups or guest wireless network.

4. Click **Apply**.

QuRouter adds the device to the blocked list.

Configuring a Device in Blocked List

1. Go to **Clients** > **Blocked List** .

2. Identity a device.

3. Click   .
   The **Edit Blocked List Device** window appears.

4. Configure the device settings.
   For details, see Adding a Device to Blocked List.

5. Click **Apply**.

QuRouter updates the device information.

Deleting a Device from Blocked List

1. Go to **Clients** > **Blocked List** .

2. Identity a device.

3. Click   .

A confirmation message appears.

4. 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. Open QuRouter.

2. Log in with your QNAP ID and password.

> **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.

3. Go to **QuWAN**.

4. 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 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.

Setting	User Action
Location	Select one of the following: • **Locate by IP address** • **Update by GPS coordinates**

5. Click **Join Organization and QuWAN**.

> ⓘ **Important**
>
> • The router is unbound from the QNAP ID once it is part of the QuWAN topology.
>
> • The router can support a maximum of 30 VPN tunnels.

A confirmation message appears.

6. Click **OK**.

QuRouter adds the router to the QuWAN topology.

Accessing QuWAN Orchestrator

1. Open QuRouter.

2.

   Click [icon] located on the task bar.

3. Click **Go to QuWAN Orchestrator**.
   QuWAN Orchestrator opens in a new browser tab.

QVPN

This section allows you to create and manage VPN servers, add VPN clients, and view VPN logs.

QVPN Settings

Enabling QBelt VPN Server

1. Open QuRouter.

2. Go to **VPN** > **VPN Settings** .

3.

   Click [toggle] .

4.

   Click [gear icon] .

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 from 10.6.0.0/24. 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)	Specify the port used to access this server. 💡 **Tip** Default port: 443
Preshared key	Specify a key (password) to verify connecting VPN clients.
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 L2TP VPN Server

1. Open QuRouter.

2. Go to **VPN** > **VPN Settings** .

3. Click ⬭ .

⊙ **Important**
You cannot enable the L2TP server if the router is using the QuWAN service.
To enable the L2TP server, you must first leave the organization and QuWAN service by clicking **Leave the organization and QuWAN** in QuWAN.

4. Click ⚙ .

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 from 10.6.0.0/24. 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
Preshared key	Specify a key (password) to verify connecting VPN clients.
DNS	Specify a DNS server for the QBelt server. **Note** The DNS server limitation is 1 by default. .

6. Click **Apply**.

QuRouter saves the L2TP server settings.

Enabling OpenVPN VPN Server

1. Open QuRouter.

2. Go to **VPN** > **VPN Settings** .

3. Click .

4. Click .

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 from 10.6.0.0/24. 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)	Specify the port used to access this server. 💡 **Tip** Default port: 443
Preshared key	Specify a key (password) to verify connecting VPN clients.
DNS	Specify a DNS server for the QBelt server. 💬 **Note** The DNS server limitation is 1 by default. .

6. Optional: Click ⬇ to download configuration files to set up a OpenVPN server manually.

7. Click **Apply**.

QuRouter saves the OpenVPN server settings.

Adding a VPN Client

1. Open QuRouter.

2. Go to **QVPN** > **Client List** .

3. Click **Add**.

4. Specify the username and password.

5. Click **Apply**.

QuRouter adds the VPN client.

QVPN Connection Logs

This screen displays a record of connections to external VPN servers. Recorded information includes the connection date, the connection duration, client name, source IP, and other detailed information.

8. Security

Security

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.
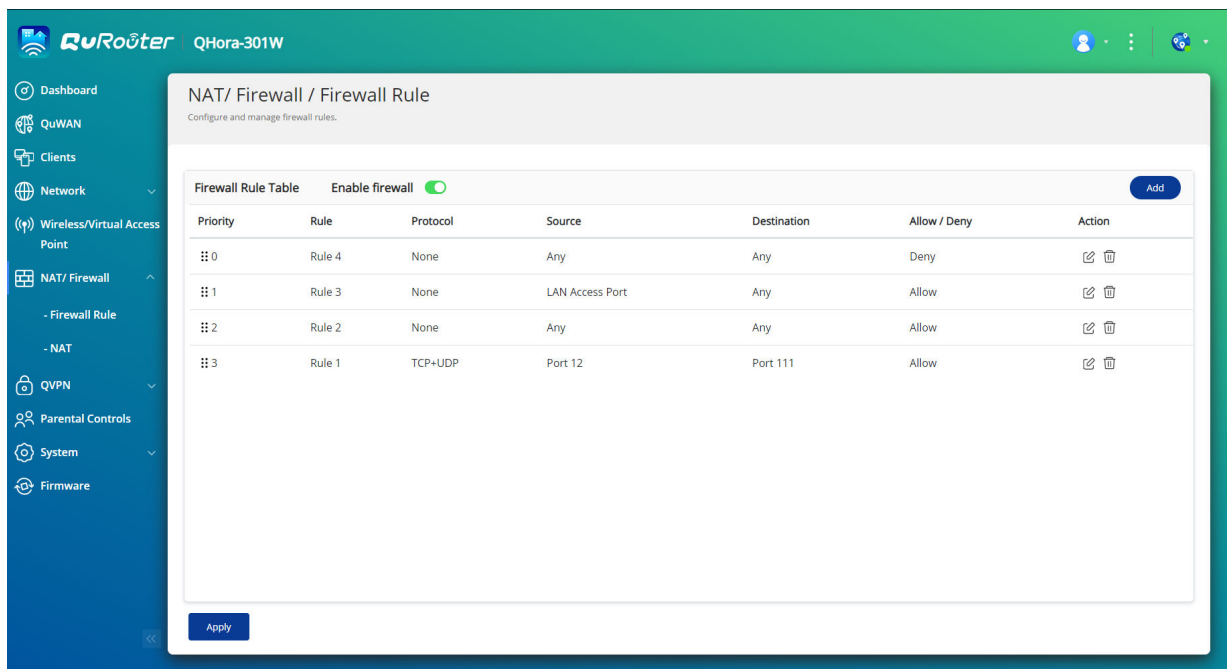
Adding a Firewall Rule

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** allows you to apply the rule to connections from an interface, a single IP, a specific subnet, or every IP within a specific range.
Port	Specify the service port for this rule. This field is only available if the **TCP** or **UDP** protocol is selected. **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.
Destination	Specify the connection destination for this rule. • Selecting **Any** applies this rule to all connections. • Selecting **Define** allows you to apply the rule to connections to a domain name, a single IP, a specific subnet, or every IP within a specific 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 the private IP addresses in the internal network into public IP address 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.

This section controls the ALG function that can be applied on the following options:

- File Transfer Protocol (FTP)

- Point-to-Point Tunneling Protocol (PPTP)

- Session Initiation Protocol (SIP)

Port Forwarding

This sections allows you to configure port forwarding rules that can be used to direct incoming and outgoing traffic on your router to a device connected on your network.
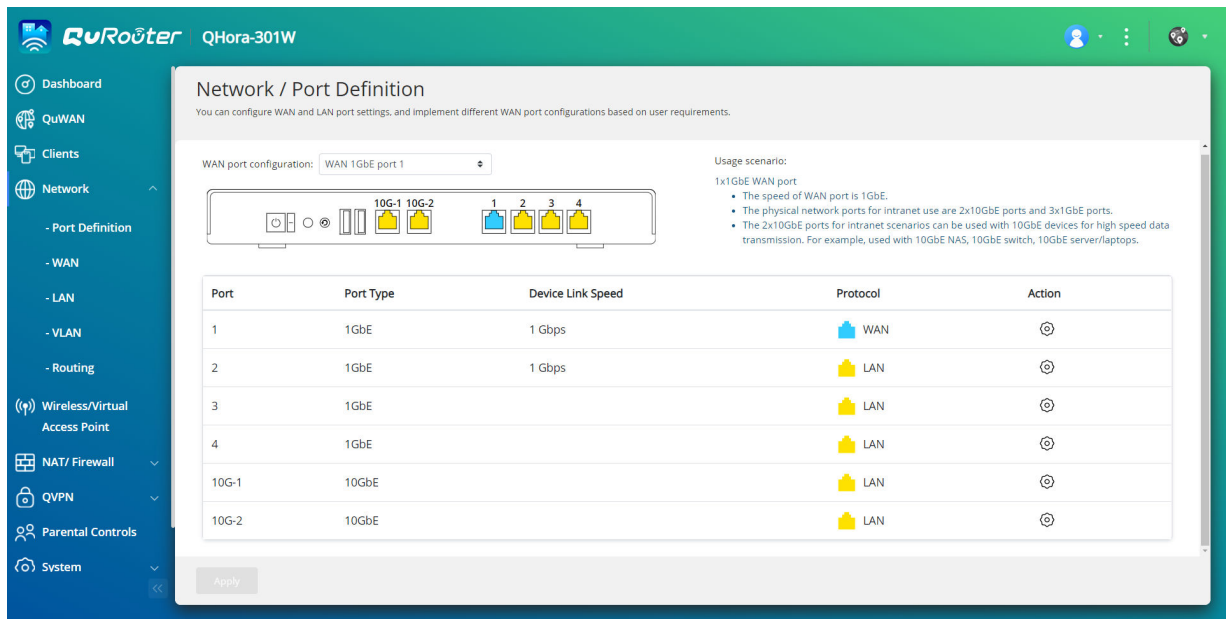
Adding a Port Forwarding Rule

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
Protocol	Select from the following options: • TCP • UDP
WAN service port	Specify the type of WAN service for the rule.
Host IP address	Specify the LAN IP address.
LAN service port	This field displays LAN service port information.
Allowed remote IPs	Specify one or more remote IP addresses. **Note** Leaving this field blank will allow access from any remote IP address.
Description	Enter a description for the rule.

4. Click **Apply**.

QuRouter adds the rule.

Configuring a Port Forwarding Rule

1. Go to **NAT/Firewall** > **NAT** > **Port Forwarding** .

2. Identify a rule.

3.

Click   .

The **Edit Rule** window appears.

4. Modify the port forwarding rule 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/Firewall** > **NAT** > **Port Forwarding** .

2. Identify a rule.

3.

Click   .

A confirmation message appears.

4. Click **Apply**.

QuRouter deletes the rule.

Parental Controls

This screen lists parental control roles. You can add, edit, or remove devices within individual parental control role.
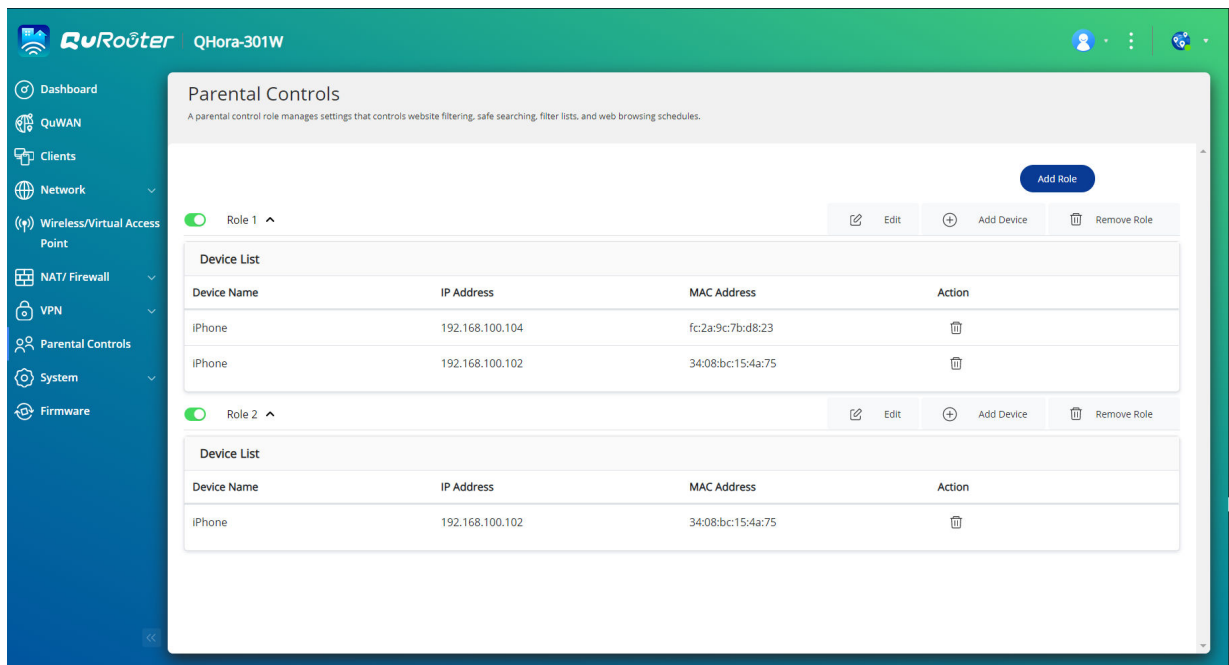
Parental control allows you to manage website filtering, safe search, and web browsing schedules.

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**
	
	    • **Medium**
	
	• **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

1. Go to **Parental Controls**.

2. Identify the role to which you want to add 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 listed in the parental control role.

3. Click 🗑 .
   A confirmation message appears.

4. Click **OK**.

QuRouter removes the device from the parental control role.

9. Support and Other Resources

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

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 QNAProuter 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.