



**QNAP**

# QHora-322

## User Guide

# Contents

<b>1. Product Overview</b>	
About the QHora-322.....	4
Hardware Specifications.....	4
Software Specifications.....	5
Package Contents.....	6
Components.....	6
Front Panel.....	7
Rear Panel.....	7
Safety Information.....	8
<b>2. Installation and Access</b>	
Installation Requirements.....	9
Setting Up the Router.....	9
Connecting the Router to the Internet.....	9
Router Access.....	11
Default Router IP Addresses.....	11
Accessing the Router Using a Browser.....	11
Accessing the Router Using Qfinder Pro.....	12
<b>3. Basic Operations</b>	
LEDs.....	13
Reset Button.....	14
<b>4. QuRouter</b>	
About QuRouter.....	15
System Requirements.....	15
Getting Started.....	15
Configuring QuRouter.....	16
Binding the Router with a QNAP ID.....	17
Unbinding the Router from a QNAP ID.....	18
<b>5. QuRouter Navigation</b>	
Taskbar.....	19
Dashboard.....	20
<b>6. System Configuration</b>	
System.....	21
System Settings.....	21
USB Settings.....	23
Managing Event Logs.....	26
Firmware.....	26
Checking for Live Updates.....	26
Updating the Firmware Manually.....	27
<b>7. Network Settings</b>	
Network.....	28
Configuring Wide Area Network (WAN) Interface Settings.....	28
Configuring Local Area Network (LAN) Interface Settings.....	30
Locating Other QNAP Devices on the Network.....	32
VLAN.....	32

Configuring the Bridge Connection Settings.....	38
Managing DHCP IP Address Reservations.....	40
Static Route.....	40
Clients.....	42
Adding a Device to the Blocked List.....	43
Configuring a Device in the Blocked List.....	43
Deleting a Device from the Blocked List.....	43
SD-WAN.....	44
About QuWAN.....	44
Configuring QuWAN Settings.....	44
Accessing QuWAN Orchestrator.....	47
Configuring the QuWAN QBelt VPN Server Settings.....	47
QVPN.....	50
QVPN Server Settings.....	50
QVPN Client Settings.....	55
Managing QVPN Logs.....	58
Service Port Management.....	58
Adding a Custom Service Port.....	58
Deleting a Custom Service Port.....	59
DDNS Settings.....	59
Configuring DDNS (My DDNS) Settings.....	59
Modifying the DDNS Domain Name.....	60

## 8. Security Settings

Firewall.....	61
Adding a Firewall Rule.....	61
Configuring a Firewall Rule.....	62
Deleting a Firewall Rule.....	63
Network Address Translation (NAT).....	63
Application Layer Gateway (ALG).....	63
Port Forwarding.....	63
Demilitarized Zone (DMZ).....	64
Web Content Filtering.....	65
Adding a Web Content Filtering Role.....	65
Configuring a Web Content Filtering Role.....	66
Deleting a Web Content Filtering Rule.....	66
Adding a Device to a Web Content Filtering Role.....	67
Deleting a Device from a Web Content Filtering Role.....	67
Quality of Service (QoS).....	67
Configuring QoS Settings on QuWAN Orchestrator.....	67

## 9. Troubleshooting

Support and Other Resources.....	70
Testing Network Connectivity with the Ping Utility.....	70
Testing Network Connectivity with the Traceroute Utility.....	70
Using QNAP Remote Support to Resolve Router Issues.....	71

## 10. Glossary

myQNAPcloud.....	73
QNAP ID.....	73
Qfinder Pro.....	73
QuRouter.....	73
QuWAN.....	73
QuWAN Orchestrator.....	73

## 11. Notices

Limited Warranty.....	74
Disclaimer.....	74
CE Notice.....	74
FCC Notice.....	75
Radio Equipment Directive (RED) 2014/53/EU Article 10.....	75
EU RoHS Statement.....	76
ISED Compliance Statement.....	76
Radiation Exposure Statement.....	76
UKCA Notice.....	76

# 1. Product Overview

This chapter provides basic information about the QNAP device.

## About the QHora-322

The QHora-322 wired router allows for high-speed network connections with six 2.5 GbE and three 10 GbE network ports. Equip your QNAP device with the router to provide secure data transmission and reduce the risk of cyber attacks. The router features built-in SD-WAN technology to support VPN deployment. 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-322
Processor	
CPU	Marvell® CN9130
Frequency	4-core 2.2 GHz
Architecture	Armv8 Cortex-A72
Memory	4GB DDR4
Flash memory	4 GB eMMC
Network	
Network interfaces	<ul style="list-style-type: none"> <li>• 6 x 2.5 GbE RJ45 (100M/1G/2.5G)</li> <li>• 3 x 10 GbE RJ45 (100M/1G/2.5/5G/10G)</li> </ul>
Maximum power consumption	36 W
External I/O Ports & Expansion Slots	
USB ports	1 x USB 3.2 Gen 1 port
Interface	
Buttons	Reset
Dimensions	
Dimensions (H x W x D)	226 x 140 x 44.4 mm (8.89 x 5.51 x 1.74 in)
Net weight	1.08 kg (2.38 lbs)
Other	
Operating temperature	0°C to 40°C (32°F to 104°F)

Component	QHora-322
Relative humidity	Non-condensing relative humidity: 5% to 95%

## Software Specifications

Specification	Description
System Status and Management	<ul style="list-style-type: none"> <li>• Connected devices</li> <li>• Device connection status</li> <li>• WAN status</li> <li>• Firmware schedule management</li> </ul>
Wired Network Management	<ul style="list-style-type: none"> <li>• Physical interface management</li> <li>• WAN interface configuration <ul style="list-style-type: none"> <li>• WAN ports</li> <li>• VLAN</li> </ul> </li> <li>• LAN interface configuration <ul style="list-style-type: none"> <li>• LAN ports</li> <li>• VLAN</li> <li>• Bridge</li> </ul> </li> <li>• Network port connection status</li> <li>• VLAN configuration</li> <li>• DHCP server configuration</li> <li>• IPv4/IPv6 routing and static route tables</li> <li>• Dynamic DNS (DDNS) configuration</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Protocol-based firewall (TCP, UDP, ICMP, TCP+UDP)</li> <li>• Firewall rules based on domain names and IP addresses</li> <li>• IP address-based firewall rule configuration</li> <li>• Network Address Translation (NAT) and port forwarding</li> <li>• Supports FTP Application-level gateway (ALG), PPTP ALG, and SIP ALG</li> <li>• Demilitarized zone (DMZ)</li> </ul>

Specification	Description
VPN	<ul style="list-style-type: none"> <li>• Remote access support using L2TP, OpenVPN, QBelt (QNAP proprietary VPN), and WireGuard protocols</li> <li>• Client IP pool management</li> <li>• VPN client management</li> <li>• Connection logs</li> <li>• Maximum VPN tunnels: 30 (including QuWAN and QVPN connections)</li> <li>• Secure remote access as VPN clients using OpenVPN protocol</li> </ul>
Access Control	Domain Name System (DNS) filtering and content filtering
System Settings	<ul style="list-style-type: none"> <li>• Backup and restore settings</li> <li>• Reset and restart settings</li> <li>• Audio alert management</li> <li>• Local account, QNAP ID, and remote management</li> <li>• USB device user management, USB usage overview, FTP server management</li> <li>• Event logs</li> </ul>
QuWAN	<ul style="list-style-type: none"> <li>• Automatic multi-site VPN configuration</li> <li>• WAN optimization                             <ul style="list-style-type: none"> <li>• WAN aggregation</li> <li>• Failover</li> <li>• Load balance</li> </ul> </li> <li>• SD-WAN management and traffic monitoring using QuWAN Orchestrator</li> <li>• Quality of Service (QoS) management</li> <li>• Maximum VPN tunnels: 30 (including QuWAN and QVPN connections)</li> <li>• 50,000 concurrent connections</li> </ul>

## Package Contents

Item	Quantity
QHora-322 router	1
Power cord	1
Quick Installation Guide (QIG)	1

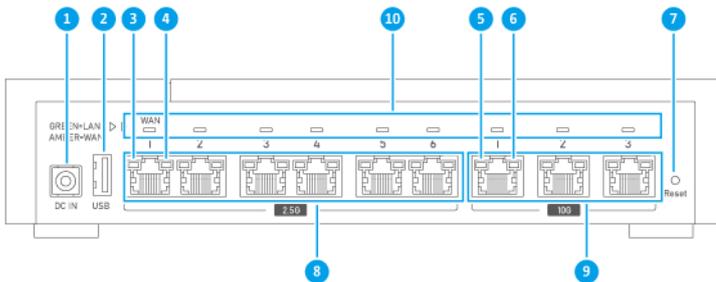
## Components

## Front Panel



No.	Component	No.	Component
1	Power LED	3	QuWAN Orchestrator status
2	System status LED	4	Auto-mesh Connection Status

## Rear Panel



No.	Component	No.	Component
1	Power input	6	10 Gigabit Ethernet LED (5 Gbps, 2.5 Gbps, 1 Gbps, or 100 Mbps speed)
2	USB 3.2 Gen 2 Type-C port	7	Reset button

No.	Component	No.	Component
3	2.5 Gigabit Ethernet LED (2.5 Gbps speed)	8	2.5 Gigabit Ethernet ports (RJ45)
4	2.5 Gigabit Ethernet LED (1 Gbps or 100 Mbps speed)	9	10 Gigabit Ethernet ports (RJ45)
5	10 Gigabit Ethernet LED (10 Gbps speed)	10	WAN and LAN LEDs

## 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.

## 2. Installation and Access

This chapter provides specific hardware installation and router access steps.

### Installation Requirements

Category	Item
Environment	<ul style="list-style-type: none"> <li>Room temperature: 0°C to 40°C (32°F to 104°F)</li> <li>Non-condensing relative humidity: 5% to 95%</li> <li>Wet-bulb temperature: 27°C (80.6°F)</li> <li>Flat, anti-static surface without exposure to direct sunlight, liquids, or chemicals</li> </ul>
Hardware and peripherals	Network cable
Tools	Anti-static wrist strap

### Setting Up the Router

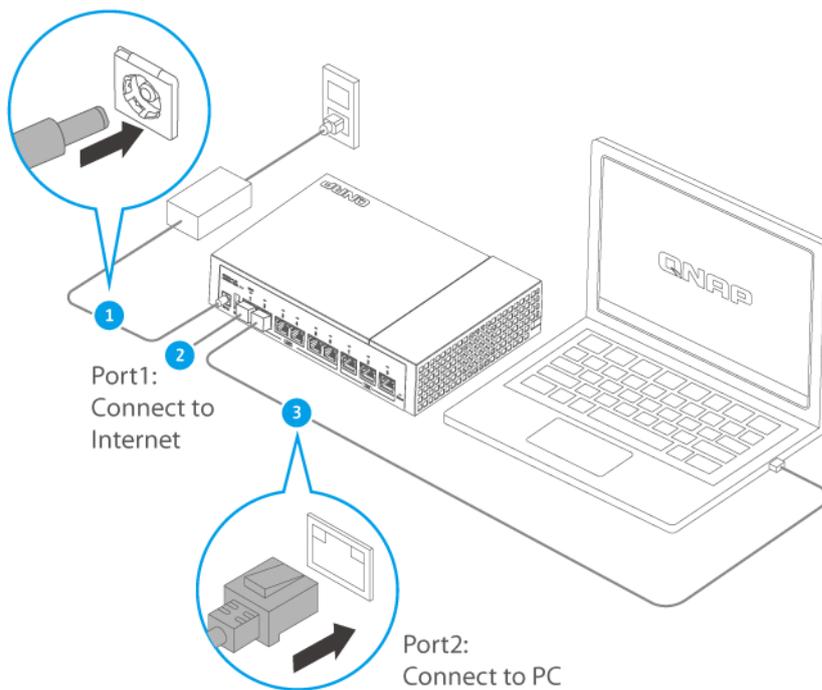
- Place your router in an environment that meets the requirements.  
For details, see [Installation Requirements](#).
- Power on the router.  
For details, see [Rear Panel](#).
- Verify the power LED is yellow-green and the system status LED is orange.  
For details, see [LEDs](#).
- Connect the router to the network and the computer.  
For details, see [Connecting the Router to the Internet](#).
- Verify that the WAN interface LED is orange and the LAN interface LED is green.  
For details, see [LEDs](#).
- 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

- Connect the router to the power source.
  - Connect the power cord to the router.
  - Connect the power adapter to the electrical outlet.

The router powers on.
- Connect the router to the internet.
  - Connect an Ethernet cable to the WAN port of the router.
  - Connect the other end of the Ethernet cable to the ISP gateway or the modem.
- Connect the router to the computer.

- a. Connect an Ethernet cable to a LAN port of the router.
- b. Connect the other end of the Ethernet cable to the Ethernet port of the computer.



### Important

The IP address to access QuRouter changes depending on which router port you connect to your computer. In the image, the computer is connected to the LAN1 interface on port 2. To access QuRouter, you must enter `192.168.100.1` in the address bar of the browser.

For details, see [Default Router IP Addresses](#).

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 on your computer.
6. Enter the router port IP address to access the QuRouter web interface.

- Follow the installation guide to configure the initial settings of the QNAP router.

## Router Access

Method	Description	Requirements
Web browser	<p>You can access the router using any computer on the same network if you have the following information:</p> <ul style="list-style-type: none"> <li>Router IP address</li> <li>Login credentials of a valid user account</li> </ul> <p>For details, see <a href="#">Accessing the Router Using a Browser</a>.</p>	<ul style="list-style-type: none"> <li>A computer connected to the same network as the router</li> <li>Web browser</li> </ul>
Qfinder Pro	<p>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.</p> <p>To download Qfinder Pro, go to <a href="https://www.qnap.com/utilities">https://www.qnap.com/utilities</a>.</p> <p>For details, see <a href="#">Accessing the Router Using Qfinder Pro</a>.</p>	<ul style="list-style-type: none"> <li>A computer connected to the same network as the router</li> <li>Web browser</li> <li>Qfinder Pro</li> </ul>

## Default Router IP Addresses

The first 2.5 GbE port is the designated WAN interface for making outbound connections. To access QuRouter, you must enter the default IP address of the LAN interface in the address bar of the browser.

By default, each LAN interface bound to a port is assigned the unique IP address listed below.

Interface Name (Port Number)	IP Address
2.5 GbE Ports	
LAN1 (Port 2)	192.168.100.1
LAN2 (Port 3)	192.168.101.1
LAN3 (Port 4)	192.168.102.1
LAN4 (Port 5)	192.168.103.1
LAN5 (Port 6)	192.168.104.1
10 GbE Ports	
LAN6 (Port 10G-1)	192.168.105.1
LAN7 (Port 10G-2)	192.168.106.1
LAN8 (Port 10G-3)	192.168.107.1

## 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.   <b>Tip</b> 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.   <b>Tip</b> 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.

### 3. Basic Operations

This chapter describes basic device operations.

#### LEDs

LEDs indicate the overall status of the router power, network ports, and system status.

LED	Status	Description
Power	Yellow-green	The router is powered on.
	Off	The router is powered off.
	Flashes yellow-green every 1 second along with the system status LED	A system error occurred.
System Status	Orange	The router is powered on and initializing.
	Flashes orange every 1 second	The router is being initialized.
	Flashes orange every 1 second along with the power LED	A system error occurred.
	Flashes orange every 2 seconds	The firmware is being updated.
	Off	The router is powered off.
QuWAN Orchestrator status	Blue-green	The router has joined the QuWAN Orchestrator topology and is connected to the SD-WAN network.
	Flashes blue-green every 0.5 seconds	The router is joining the QuWAN Orchestrator SD-WAN network.
	Flashes blue-green every 2 seconds	The router lost connection to the QuWAN Orchestrator SD-WAN network.
	Off	The router is not part of the QuWAN Orchestrator SD-WAN network.
Auto-mesh Connection Status	White	Connected: All the mesh VPN tunnels established by the device on the QuWAN Orchestrator SD-WAN network are accessible.
	Flashes white every 2 seconds	Partially connected: Few of the mesh VPN tunnels established by the router on the QuWAN Orchestrator SD-WAN network are inaccessible.
	Off	The router is not part of the QuWAN Orchestrator SD-WAN network.
2.5 Gigabit Ethernet (2.5 Gbps speed)	Green	The network connection is operating at 2.5 Gbps.
	Flashes green	Data is being transmitted.
	Off	There is no network connection.

LED	Status	Description
2.5 Gigabit Ethernet (1 Gbps or 100 Mbps speed)	Orange	The network connection is operating at 1 Gbps or 100 Mbps.
	Flashes orange	Data is being transmitted.
	Off	There is no network connection.
10 Gigabit Ethernet (10 Gbps speed)	Green	The network connection is operating at 10 Gbps.
	Flashes green	Data is being transmitted.
	Off	There is no network connection.
10 Gigabit Ethernet (5 Gbps, 2.5 Gbps, 1 Gbps, or 100 Mbps)	Orange	The network connection is operating at 5 Gbps, 2.5 Gbps, 1 Gbps, or 100 Mbps.
	Flashes orange	Data is being transmitted.
	Off	There is no network connection.
2.5 Gigabit Ethernet WAN	Orange	A WAN connection has been established.
2.5 Gigabit Ethernet LAN	Green	A LAN connection has been established.
10 Gigabit Ethernet WAN	Orange	A WAN connection has been established.
10 Gigabit Ethernet LAN	Green	A LAN connection has been established.

## 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.

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.

## 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	<ul style="list-style-type: none"> <li>• Web browser:               <ul style="list-style-type: none"> <li>• Microsoft Edge 42 or later</li> <li>• Mozilla Firefox 60.0 or later</li> <li>• Apple Safari 11.1 or later</li> <li>• Google Chrome 70.0 or later</li> </ul> </li> <li>• Qfinder Pro 6.9.2 or later</li> </ul>

### 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 [Network Settings](#).
3. 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](#)
4. 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 the default IP address of the network interface in the address bar.



### Important

The IP address to access QuRouter changes depending on the which router port is connected to your computer.

For details, see [Default Router IP Addresses](#).

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.



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
<b>DHCP</b>	Obtain IP address settings automatically via DHCP
<b>Static IP</b>	Manually assign a static IP address. You must specify the following information: <ul style="list-style-type: none"> <li>• Fixed IP address</li> <li>• Subnet mask</li> <li>• DNS server</li> </ul>
<b>PPPoE</b>	Select this option to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

11. Click **Apply**.
12. Update the firmware to the latest version.  
For details, see the [Firmware](#) section.
13. Click **Apply**.
14. Enter the default username and password.

Default Username	Default Password
admin	QuRouter: The router MAC address without any punctuation and all letters capitalized.   <b>Tip</b> 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.

15. Click **Login**.  
The **Local Account** window appears.
16. Optional: You can log in to QuRouter using your QNAP ID and password.  
For details, see [Binding the Router with a QNAP ID](#).
17. Reenter or modify the local account username and password.
18. Click **OK**.  
A confirmation message appears.

QuRouter saves the settings.

## 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.

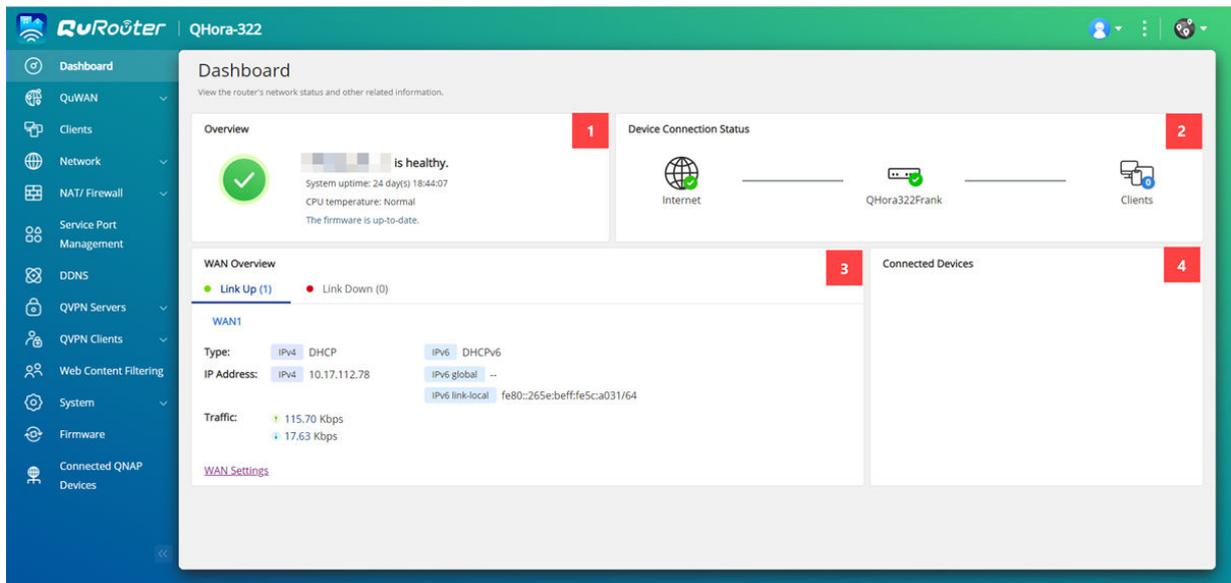
## 5. QuRouter Navigation

### Taskbar



No.	Element	User Action
1	[USER_NAME]	<b>Logout:</b> Logs the user out of the current session
2	<b>More</b>	<p>Click the button to view the following menu items:</p> <ul style="list-style-type: none"> <li>• <b>Language:</b> Opens a list of supported languages and allows you to change the language of the operating system</li> <li>• <b>Domain Settings:</b> Click to change the domain.</li> </ul> <p><b>Note</b>                      You cannot change the domain if the router was previously added to the QuWAN network.</p> <ul style="list-style-type: none"> <li>• <b>About:</b> Displays the following information:                             <ul style="list-style-type: none"> <li>• Operating system</li> <li>• Hardware model</li> <li>• Firmware version</li> </ul> </li> <li>• <b>QNAP Remote Support:</b> Click to create a support ticket and contact the QNAP Customer Service team.                              For details, see <a href="#">Using QNAP Remote Support to Resolve Router Issues</a>.</li> </ul>
3	QuWAN	<p>Click the button to view QuWAN-related information.</p> <ul style="list-style-type: none"> <li>• QuWAN Orchestrator connection status</li> <li>• Organization</li> <li>• QuWAN settings</li> <li>• Link to QuWAN Orchestrator</li> </ul>

## Dashboard



No.	Section	Displayed Information	User Action
1	Overview	<ul style="list-style-type: none"> <li>System uptime (number of days, hours, minutes, and seconds)</li> <li>CPU temperature</li> <li>Firmware information</li> </ul>	-
2	Device Connection Status	<ul style="list-style-type: none"> <li>Internet status</li> <li>Device status</li> <li>Number of connected clients</li> </ul>	-
3	WAN Overview	<ul style="list-style-type: none"> <li>Link up and link down information</li> <li>Connection type</li> <li>IP address information</li> <li>Traffic information</li> </ul>	Click <b>WAN Settings</b> to open <b>Network &gt; Physical Interface Settings</b> .
4	Connected Devices	Names of the connected QNAP devices	Click <b>Connected QNAP Devices</b> to view QNAP devices on the same network subnet.

## 6. System Configuration

### System

#### 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**

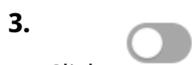
If the selected backup file contains user or user group information that already exists on the device, the system will overwrite the existing information.

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** .



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
<b>Local management via HTTP</b>	Enable to allow local access to the router web interface using non-HTTPS connections.  <b>Note</b> HTTP connections are faster than Hypertext Transfer Protocol Secure (HTTPS); however, the transferred content is not encrypted.
<b>Remote management</b>	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.  Under Local Account, click  . The **Local Account** window appears.
4. Configure the local account settings.

Description	User Action
New 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 **Apply**.

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.   <b>Note</b> QuRouter allows up to 9 concurrent connections.
File name encoding	Select from the following options:  <ul style="list-style-type: none"> <li>• <b>utf-8</b></li> <li>• <b>big5</b></li> </ul>

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 interface.  
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 interface.

### 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.  <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Passwords are case-sensitive.</li> <li>• Click  to make the password visible.</li> </ul> </div> </div>

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 (_)  <div style="display: flex; align-items: center;">  <div> <p><b>Note</b></p> <p>The .pcap file is automatically stored in the USB device that is connected to the router.</p> </div> </div>
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.

## 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.

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.
ℹ	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.
ℹ	2020-12-18 10:10:41	192.168.100.101	General	[QuRouter] User "admin" logged in.
ℹ	2020-12-18 10:09:12	192.168.100.101	system	[QuRouter] Configured primary device "Office".
ℹ	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
ℹ	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
ℹ	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)

## 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

#### Configuring Wide Area Network (WAN) Interface Settings

1. Log in to QuRouter
2. Go to **Network > Physical Interface Settings > WAN** .
3. Identify a WAN interface.
4.  Click  .  
The port configuration window appears.
5. Select **WAN** as the interface.
6. Configure the interface settings.

Setting	User Action
Interface name	Specify an interface name between 1 and 64 characters.
Description (optional)	Enter a description for the interface.
MTU	Specify an MTU value between 576 and 1500.   <b>Note</b> The Maximum Transmission Unit (MTU) is the largest packet size that is transmitted by a network.
Transferring (Tx) ISP line rate	Specify the gross transmitting bit rate of the physical layer.   <b>Note</b> You can set the ISP line rate only if you have configured the QuWAN and QoS settings.
Receiving (Rx) ISP line rate	Specify the gross receiving bit rate of the physical layer.

7. Configure the IPv4 address assignment settings.
  - a. Select the interface connection from the following options.

Setting	Description
<b>DHCP</b>	Obtain IP address settings automatically via DHCP
<b>Static IP</b>	Manually assign a static IP address. You must specify the following information: <ul style="list-style-type: none"> <li>• Fixed IP Address</li> <li>• Subnet Mask</li> <li>• Default Gateway</li> <li>• Primary and secondary DNS servers</li> </ul>
<b>PPPoE</b>	Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

b. Configure the DNS settings.

Setting	Description
DNS server	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> Automatically obtain the IP address using DHCP.</li> <li>• <b>Manually:</b> Manually assign the IP address for the primary and secondary DNS servers.</li> </ul> <p> <b>Important</b> QNAP recommends specifying at least one DNS server to allow URL lookups.</p>

8. Configure the IPv6 settings.

a. Click **Enable IPv6**.

b. Configure the connection settings.

Setting	User Action
<b>DHCPv6</b>	<p>The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.</p> <p> <b>Important</b> This option requires an available DHCPv6-enabled server on the network.</p>
<b>Static IP</b>	<p>Manually assign a static IP address to the adapter. You must specify the following information:</p> <ul style="list-style-type: none"> <li>• Fixed IP Address</li> <li>• Prefix length</li> </ul> <p> <b>Tip</b> Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> <li>• Default Gateway</li> <li>• Primary and secondary DNS servers</li> </ul>
<b>PPPoEv6</b>	<p>Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE) IPv6 protocol.</p> <p> <b>Important</b> You must change the IPv4 WAN interface to PPPoE if you want to use PPPoEv6 as the WAN interface.</p>
<b>Stateless (SLAAC)</b>	<p>The adapter automatically acquires an IPv6 address and DNS settings from the router.</p> <p> <b>Important</b> This option requires an available IPv6 RA (router advertisement)-enabled router on the network.</p>

c. Click **DHCPv6 prefix delegation (DHCPv6 PD)** to provide IPv6 addresses on the subscriber LAN.



**Note**

Prefix delegation is available only for PPPoEv6 and Stateless (SLAAC) options.

9. Click **Apply**.

QuRouter updates the WAN settings.

## Configuring Local Area Network (LAN) Interface Settings

1. Log in to QuRouter
2. Go to **Network > Physical Interface Settings > LAN** .
3. Identify a LAN interface.
4.  Click  .  
The port configuration window appears.
5. Select **LAN** as the interface.
6. Configure the interface settings.

Setting	User Action
Interface name	Specify an interface name between 1 and 64 characters.
Description (optional)	Enter a description for the interface.
MTU	Specify an MTU value between 576 and 9000.   <b>Note</b> The Maximum Transmission Unit (MTU) is the largest packet size that is transmitted by a network.

7. Configure the IPv4 address assignment settings.

Setting	User Action
<b>Fixed IP address</b>	Specify a fixed IP address.   <b>Tip</b> Examine your network setup for guidance on how to best configure these settings.
<b>Subnet Mask</b>	Specify the subnet mask used to subdivide your IP address.
<b>Enable Spanning Tree Protocol (STP)</b>	Enable to prevent network loops.

Setting	User Action
<p><b>Enable DHCP server</b></p>	<p>Configure the DHCP server settings.</p> <ul style="list-style-type: none"> <li>• <b>Start IP address:</b> Specify the starting IP address in a range allocated to DHCP clients.</li> <li>• <b>End IP address:</b> Specify the ending IP address in a range allocated to DHCP clients.</li> <li>• <b>Lease time:</b> 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.</li> <li>• Configure the DNS server settings:                             <ul style="list-style-type: none"> <li>• <b>Use the fixed IP address:</b> Select to use the same IP address assigned for the fixed IP address.</li> <li>• <b>Manually:</b> Manually configure the DNS server IP addresses.</li> </ul> </li> </ul> <p> <b>Note</b> QNAP recommends specifying at least one DNS server to allow URL lookups.</p>
<p><b>Reserved IP Table</b></p>	<ul style="list-style-type: none"> <li>• Click <b>Add</b> to configure a reserved IP table.</li> <li>• Specify the following:                             <ul style="list-style-type: none"> <li>• Device name</li> <li>• IP address</li> <li>• MAC address</li> </ul> </li> <li>• Click  .</li> </ul>

8. Configure the IPv6 address assignment settings.
  - a. Click **IPv6**.
  - b. Click **Enable IPv6**.
  - 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
<p>Interface identifier</p>	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>EUI-64:</b> Select Extended Unique Identifier (EUI-64) to automatically configure IPv6 host address.</li> <li>• <b>Manually:</b> Specify an interface ID to configure the IPv6 host address.</li> </ul>

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

Setting	Description
IPv6 addressing mode	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>Stateful:</b> The stateful DHCPv6 or managed mode enables you to manually assign a unique IPv6 address to each client.</li> <li>• <b>Stateless:</b> 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.</li> <li>• <b>SLAAC+RDNSS:</b> Stateless Address Auto-Configuration (SLAAC) along with Recursive DNS Server (RDNSS) enables users to manually assign an IP address based on the IPv6 prefix and uses recursive queries to resolve the domain name.</li> <li>• <b>Disabled:</b> Disables IPv6 client addressing.</li> </ul>

9. Click **Apply**.

QuRouter updates the LAN settings.

### Locating Other QNAP Devices on the Network

Your router can find other QNAP devices connected to the same network subnet.

1. Log in to QuRouter.
2. Go to **Connected QNAP Devices**.
3. Perform any of the following actions.

Task	User Action
Locate a device	<p><b>a.</b> Type the keywords in the search field.</p> <p><b>b.</b> Press <b>Enter</b>.</p>
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 WAN VLAN Interface

1. Log in to QuRouter.
2. Go to **Network > VLAN Settings > VLAN Settings**.
3. Click **Add VLAN**.  
The **VLAN Configuration** window opens.

4. Select **WAN** as the interface.
5. Configure the interface settings.

Setting	User Action
Interface name	Specify an interface name between 1 and 64 characters.
Description (optional)	Enter a description for the interface.
MTU	Specify an MTU value between 576 and 1500.   <b>Note</b> The Maximum Transmission Unit (MTU) is the largest packet size that is transmitted by a network.
Transferring (Tx) ISP line rate	Specify the gross transmitting bit rate of the physical layer.   <b>Note</b> You can set the ISP line rate only if you have configured the QuWAN and QoS settings.
Receiving (Rx) ISP line rate	Specify the gross receiving bit rate of the physical layer.   <b>Note</b> You can set the ISP line rate only if you have configured the QuWAN and QoS settings.

6. Configure the tagged or untagged member port of the VLAN.
7. Configure the IPv4 address assignment settings.
  - a. Select the interface connection from the following options.

Setting	Description
<b>DHCP</b>	Obtain IP address settings automatically via DHCP
<b>Static IP</b>	Manually assign a static IP address. You must specify the following information: <ul style="list-style-type: none"> <li>• Fixed IP Address</li> <li>• Subnet Mask</li> <li>• Default Gateway</li> <li>• Primary and secondary DNS servers</li> </ul>
<b>PPPoE</b>	Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE).

- b. Configure the DNS settings.

Setting	Description
DNS server	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> Automatically obtain the IP address using DHCP.</li> <li>• <b>Manually:</b> Manually assign the IP address for the primary and secondary DNS servers.</li> </ul> <p> <b>Important</b> QNAP recommends specifying at least one DNS server to allow URL lookups.</p>

8. Configure the IPv6 settings.

- a. Click **Enable IPv6**.
- b. Configure the connection settings.

Setting	User Action
<b>DHCPv6</b>	<p>The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.</p> <p> <b>Important</b> This option requires an available DHCPv6-enabled server on the network.</p>
<b>Static IP</b>	<p>Manually assign a static IP address to the adapter. You must specify the following information:</p> <ul style="list-style-type: none"> <li>• Fixed IP Address</li> <li>• Prefix length</li> </ul> <p> <b>Tip</b> Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> <li>• Default Gateway</li> <li>• Primary and secondary DNS servers</li> </ul>
<b>PPPoEv6</b>	<p>Select to specify a username and password for Point-to-Point Protocol over Ethernet (PPPoE) IPv6 protocol.</p> <p> <b>Important</b> You must change the IPv4 WAN interface to PPPoE if you want to use PPPoEv6 as the WAN interface.</p>
<b>Stateless (SLAAC)</b>	<p>The adapter automatically acquires an IPv6 address and DNS settings from the router.</p> <p> <b>Important</b> This option requires an available IPv6 RA (router advertisement)-enabled router on the network.</p>

- c. Click **DHCPv6 prefix delegation (DHCPv6 PD)** to provide IPv6 addresses on the subscriber LAN.



**Note**

Prefix delegation is available only for PPPoEv6 and Stateless (SLAAC) options.

9. Click **Apply**.

QuRouter adds the WAN VLAN interface.

### Adding a LAN VLAN Interface

1. Log in to QuRouter
2. Go to **Network > VLAN Settings > VLAN Settings** .
3. Click **Add VLAN**.  
The **VLAN Configuration** window opens.
4. Select **LAN** as the interface.
5. Configure the interface settings.

Setting	User Action
Interface name	Specify an interface name between 1 and 64 characters.
Description (optional)	Enter a description for the interface.
MTU	Specify an MTU value between 576 and 9000.   <b>Note</b> The Maximum Transmission Unit (MTU) is the largest packet size that is transmitted by a network.

6. Configure the tagged and untagged member ports of the VLAN.
7. Configure the IPv4 address assignment settings.

Setting	User Action
<b>Fixed IP address</b>	Specify a fixed IP address.   <b>Tip</b> Examine your network setup for guidance on how to best configure these settings.
<b>Subnet Mask</b>	Specify the subnet mask used to subdivide your IP address.
<b>Enable Spanning Tree Protocol (STP)</b>	Enable to prevent network loops.

Setting	User Action
<p><b>Enable DHCP server</b></p>	<p>Configure the DHCP server settings.</p> <ul style="list-style-type: none"> <li>• <b>Start IP address:</b> Specify the starting IP address in a range allocated to DHCP clients.</li> <li>• <b>End IP address:</b> Specify the ending IP address in a range allocated to DHCP clients.</li> <li>• <b>Lease time:</b> 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.</li> <li>• Configure the DNS server settings:                             <ul style="list-style-type: none"> <li>• <b>Use the fixed IP address:</b> Select to use the same IP address assigned for the fixed IP address.</li> <li>• <b>Manually:</b> Manually configure the DNS server IP addresses.</li> </ul> </li> </ul> <p> <b>Note</b> QNAP recommends specifying at least one DNS server to allow URL lookups.</p>
<p><b>Reserved IP Table</b></p>	<ul style="list-style-type: none"> <li>• Click <b>Add</b> to configure a reserved IP table.</li> <li>• Specify the following:                             <ul style="list-style-type: none"> <li>• Device name</li> <li>• IP address</li> <li>• MAC address</li> </ul> </li> <li>• Click  .</li> </ul>

8. Configure the IPv6 address assignment settings.
  - a. Click **IPv6**.
  - b. Click **Enable IPv6**.
  - 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
<p>Interface identifier</p>	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>EUI-64:</b> Select Extended Unique Identifier (EUI-64) to automatically configure IPv6 host address.</li> <li>• <b>Manually:</b> Specify an interface ID to configure the IPv6 host address.</li> </ul>

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

Setting	Description
IPv6 addressing mode	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>Stateful:</b> The stateful DHCPv6 or managed mode enables you to manually assign a unique IPv6 address to each client.</li> <li>• <b>Stateless:</b> 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.</li> <li>• <b>SLAAC+RDNSS:</b> Stateless Address Auto-Configuration (SLAAC) along with Recursive DNS Server (RDNSS) enables users to manually assign an IP address based on the IPv6 prefix and uses recursive queries to resolve the domain name.</li> <li>• <b>Disabled:</b> Disables IPv6 client addressing.</li> </ul>

9. Click **Apply**.

QuRouter adds the VLAN LAN interface.

### Configuring VLAN Settings

1. Log in to QuRouter.
2. Go to **Network > VLAN Settings > VLAN 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 the following:

- [Adding a WAN VLAN Interface](#)
- [Adding a LAN VLAN Interface](#)

6. Click **Apply**.

QuRouter updates the VLAN settings.

### Deleting a VLAN

1. Log in to QuRouter.
2. Go to **Network > VLAN Settings > VLAN Settings** .
3. Identify the VLAN.
4.  Click  . A confirmation message appears.
5. Click **Yes**.

QuRouter deletes the VLAN.

## Configuring the Bridge Connection Settings

Your router can be configured to create a wired bridge to provide a transparent connection to all the devices in the network. Bridge mode allows you to connect two routers without any IP address conflict and extend port availability to several devices.



### Important

To create a wired bridge connection between the two routers, make sure you configure the same settings on both routers.

1. Log in to QuRouter
2. Go to **Network > Bridge** .
3. Click **Add Bridge**.  
The **Bridge** window appears.
4. Enter a description for the interface.
5. Specify an MTU value between 576 and 9000.
6. Select one or more available interfaces from the list.
7. Click  .  
QuRouter adds the interfaces to the bridge connection list.



### Note

Click  to remove the added interfaces from the list.

8. Configure the IPv4 address assignment settings.

Setting	User Action
<b>Fixed IP address</b>	Specify a fixed IP address.   <b>Tip</b> Examine your network setup for guidance on how to best configure these settings.
<b>Subnet Mask</b>	Specify the subnet mask used to subdivide your IP address.
<b>Enable Spanning Tree Protocol (STP)</b>	Enable to prevent network loops.

Setting	User Action
<p><b>Enable DHCP server</b></p>	<p>Configure the DHCP server settings.</p> <ul style="list-style-type: none"> <li>• <b>Start IP address:</b> Specify the starting IP address in a range allocated to DHCP clients.</li> <li>• <b>End IP address:</b> Specify the ending IP address in a range allocated to DHCP clients.</li> <li>• <b>Lease time:</b> 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.</li> <li>• Configure the DNS server settings:                             <ul style="list-style-type: none"> <li>• <b>Use the fixed IP address:</b> Select to use the same IP address assigned for the fixed IP address.</li> <li>• <b>Manually:</b> Manually configure the DNS server IP addresses.</li> </ul> </li> </ul> <p> <b>Note</b> QNAP recommends specifying at least one DNS server to allow URL lookups.</p>
<p><b>Reserved IP Table</b></p>	<ul style="list-style-type: none"> <li>• Click <b>Add</b> to configure a reserved IP table.</li> <li>• Specify the following:                             <ul style="list-style-type: none"> <li>• Device name</li> <li>• IP address</li> <li>• MAC address</li> </ul> </li> <li>• Click  .</li> </ul>

9. Configure the IPv6 address assignment settings.
  - a. Click **IPv6**.
  - b. Click **Enable IPv6**.
  - 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
<p>Interface identifier</p>	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>EUI-64:</b> Select Extended Unique Identifier (EUI-64) to automatically configure IPv6 host address.</li> <li>• <b>Manually:</b> Specify an interface ID to configure the IPv6 host address.</li> </ul>

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

Setting	Description
IPv6 addressing mode	<p>Select from the following:</p> <ul style="list-style-type: none"> <li>• <b>Stateful:</b> The stateful DHCPv6 or managed mode enables you to manually assign a unique IPv6 address to each client.</li> <li>• <b>Stateless:</b> 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.</li> <li>• <b>SLAAC+RDNSS:</b> Stateless Address Auto-Configuration (SLAAC) along with Recursive DNS Server (RDNSS) enables users to manually assign an IP address based on the IPv6 prefix and uses recursive queries to resolve the domain name.</li> <li>• <b>Disabled:</b> Disables IPv6 client addressing.</li> </ul>

10. Click **Apply**.

QuRouter adds the bridge connection.

## Managing DHCP IP Address Reservations

To ensure that a network interface receives the same IP address every time your router is rebooted, you can reserve the IP address provided by the DHCP server.

1. Log in to QuRouter.
2. Go to **Network > DHCP Table**.
3. Select one or more interfaces.
4. Click **Reserve**.



### Tip

To unreserve DHCP IP addresses for the selected interfaces, click **Unreserve**.

QuRouter reserves DHCP IP addresses for the selected interfaces.

## 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
<b>Destination</b>	Specify a static IP address where connections are routed to.
<b>Subnet Mask</b>	Specify the IP address of the destination's subnet mask.
<b>Next Hop</b>	Select from the following next hop options: <ul style="list-style-type: none"> <li>• <b>WAN Interface:</b> Select an available WAN interface for the routing path.</li> <li>• <b>IP Address:</b> Specify the IP address of the closest or most optimal router in the routing path.</li> </ul>
<b>Metric</b>	Specify the number of nodes that the route will pass through. <div style="border-left: 2px solid #007bff; padding-left: 10px; margin-top: 10px;">  <b>Note</b> Metrics are cost values used by routers to determine the best path to a destination network.                     </div>
<b>Description</b>	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
<b>Destination</b>	Specify a static IP address where connections are routed to.
<b>Prefix length</b>	Select the prefix length for IPv6 addressing.
<b>Next Hop</b>	Select an available WAN interface for the routing path.
<b>Metric</b>	Specify the number of nodes that the route will pass through. <div style="border-left: 2px solid #007bff; padding-left: 10px; margin-top: 10px;">  <b>Note</b> Metrics are cost values used by routers to determine the best path to a destination network.                     </div>
<b>Description</b>	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.

## Clients

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

Additionally, you can use the Blocked list to control the management of any clients blocked from accessing the network 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.   <b>Note</b> <ul style="list-style-type: none"> <li>• The description must be between 1 to 20 characters.</li> <li>• Valid characters: A-Z, a-z, 0-9</li> <li>• Valid special characters: Hyphen (-), Underscore (_), Period (.)</li> </ul>
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. Identify 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

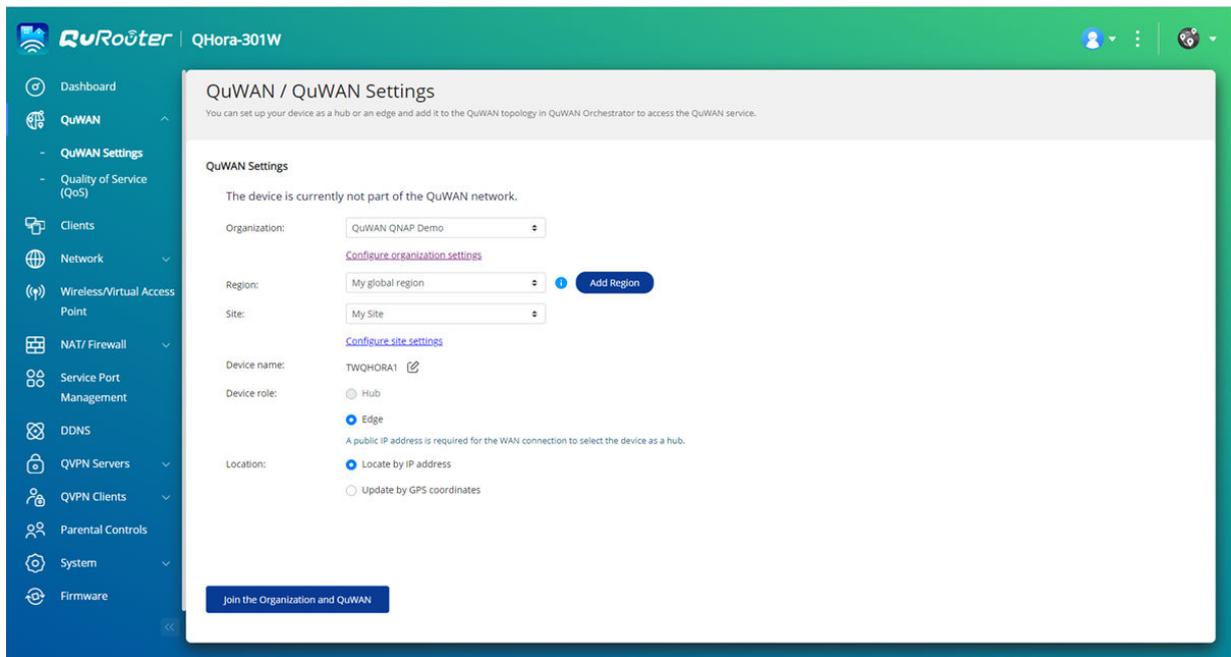
If you are logging in with your QNAP ID for the first time, you are prompted to enter the local account credentials as part of the 2-step verification process.



#### 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	<p>Select an organization associated with your QNAP ID.</p> <p><b>Note</b> If there are no organizations associated with your QNAP ID, click <b>Create or edit organization</b>. QuRouter redirects you to QNAP Account website where you can create a new organization or edit an existing one.</p>
Region	<p>Select a region linked with the selected organization. Click <b>Add Region</b> to create a new region.</p>
Site	<p>Select a site from the drop-down menu.</p> <p><b>Note</b> Click <b>Create or edit site</b> to create a new site associated with the selected organization or edit an existing site.</p>
Device name	<p>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</p>

Setting	User Action
Device role	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Hub:</b> 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.</li> <li>• <b>Edge:</b> Configure the device as an SD-WAN edge.</li> </ul> <p> <b>Important</b></p> <ul style="list-style-type: none"> <li>• You can only assign the device role of edge to devices behind NAT in an organization.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Location	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Locate by IP address</b></li> <li>• <b>Update by GPS coordinates</b></li> </ul>

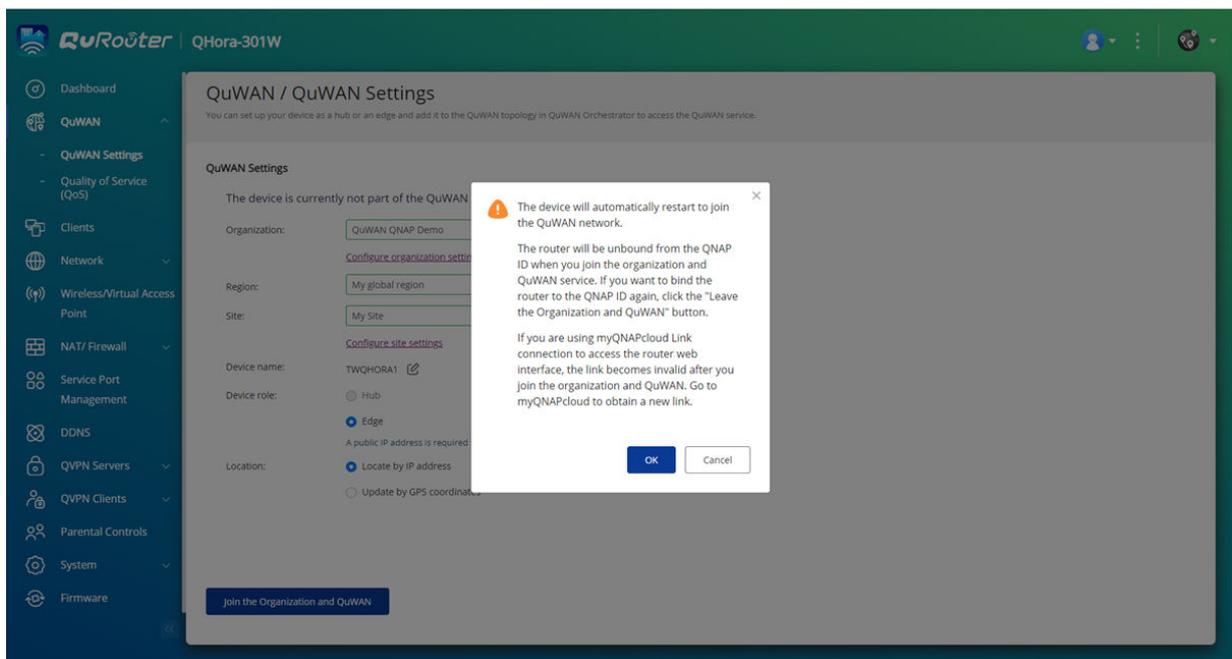
#### 4. Click **Join the Organization and QuWAN**.



#### **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.

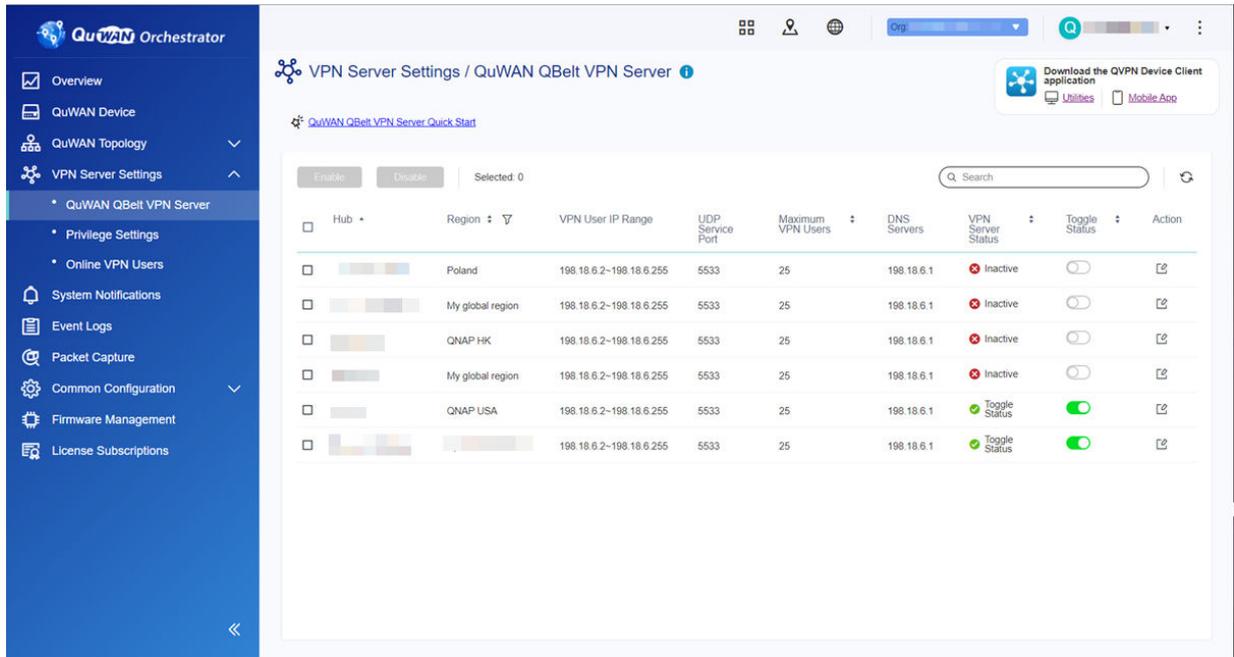
2. Go to **QuWAN > QuWAN QBelt VPN Server**.

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** .



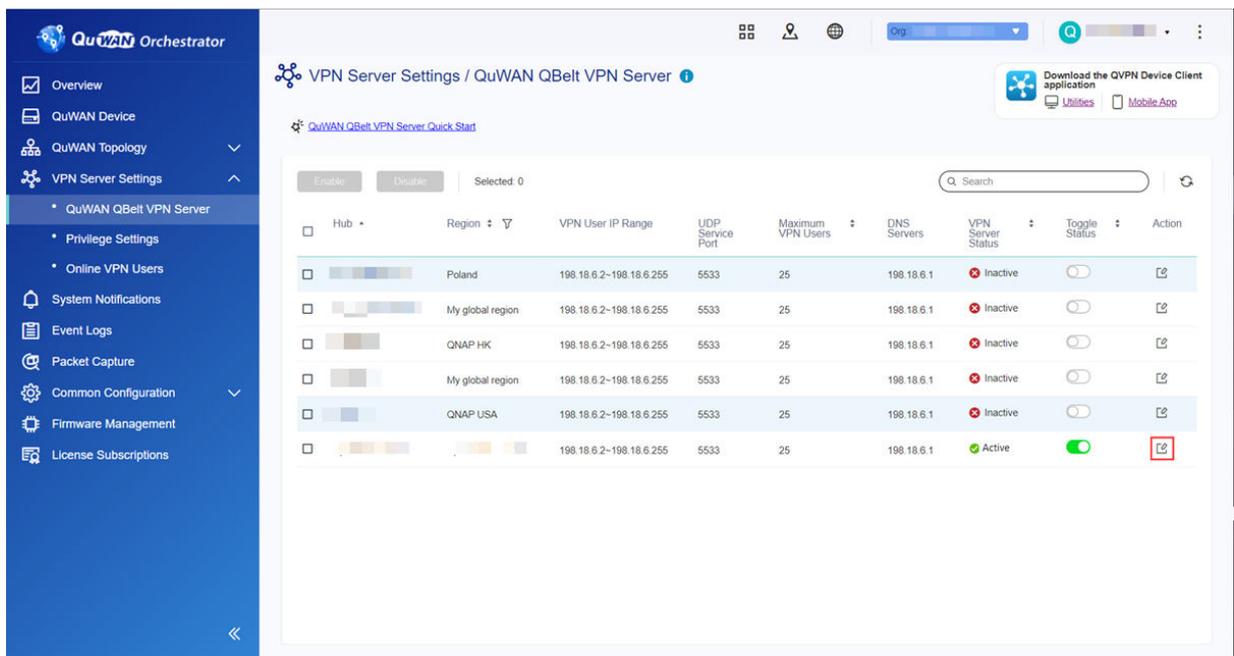
6. Identify a hub.

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.

### Configure "quwan" VPN Server Settings

✕

\* Required field

Region: QNAP USA

VPN User IP range: \*  .  .  . 2

Subnet mask: \*

UDP service port: 5533 | [Service Management](#)

Maximum VPN Users \*

DNS servers: \*  (DNS limitation: 3)

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	<p>Click <b>Service Management</b> to assign a port number for the UDP service port.</p> <p> <b>Tip</b> Click  to refresh the UDP service port number.</p>
Maximum number of VPN users	<p>Specify the maximum number of VPN users that can connect to the VPN server.</p> <p> <b>Note</b> The maximum value you can enter depends on the specified subnet mask.</p>
DNS servers	<p>Specify the IP address of the DNS servers.</p> <p> <b>Tip</b></p> <ul style="list-style-type: none"> <li>• You can specify up to three DNS servers.</li> <li>• Separate entries with a comma (,).</li> </ul>

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
<b>Client IP pool</b>	Specify a range of IP addresses available to connected VPN clients.   <b>Important</b> 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.
<b>Service Port (UDP)</b>	Select the port used to access the server.   <b>Note</b> Default port number: 4433

Setting	Description
<b>Pre-shared key</b>	Specify a pre-shared key (password) to verify connecting VPN clients.   <b>Tip</b> Pre-shared key requirements: <ul style="list-style-type: none"> <li>• Length: 8–16 ASCII characters</li> <li>• Valid characters: A–Z, a–z, 0–9</li> </ul>
<b>DNS</b>	Specify a DNS server for the QBelt server.   <b>Note</b> 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
<b>Client IP pool</b>	Specify a range of IP addresses available to connected VPN clients.   <b>Important</b> 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.
<b>Authentication</b>	Select one of the following authentication methods: <ul style="list-style-type: none"> <li>• <b>PAP</b></li> <li>• <b>MS-CHAPv2</b></li> </ul>

Setting	Description
<b>Pre-shared key</b>	Specify a pre-shared key (password) to verify connecting VPN clients.   <b>Tip</b> Pre-shared key requirements: <ul style="list-style-type: none"> <li>• Length: 8–16 ASCII characters</li> <li>• Valid characters: A–Z, a–z, 0–9</li> </ul>
<b>DNS</b>	Specify a DNS server for the L2TP server.   <b>Note</b> 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
<b>Client IP pool</b>	Specify a range of IP addresses available to connected VPN clients.   <b>Important</b> 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.
<b>Service Port</b>	Select from the following options: <ul style="list-style-type: none"> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> </ul>  <b>Note</b> Default port number: 1194

Setting	Description
<b>Encryption</b>	Select from the following encryption methods: <ul style="list-style-type: none"> <li>• <b>Medium (AES 128-bit)</b></li> <li>• <b>High (AES 256-bit)</b></li> </ul>
<b>DNS</b>	Specify a DNS server for the OpenVPN server.  <b>Note</b> 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.

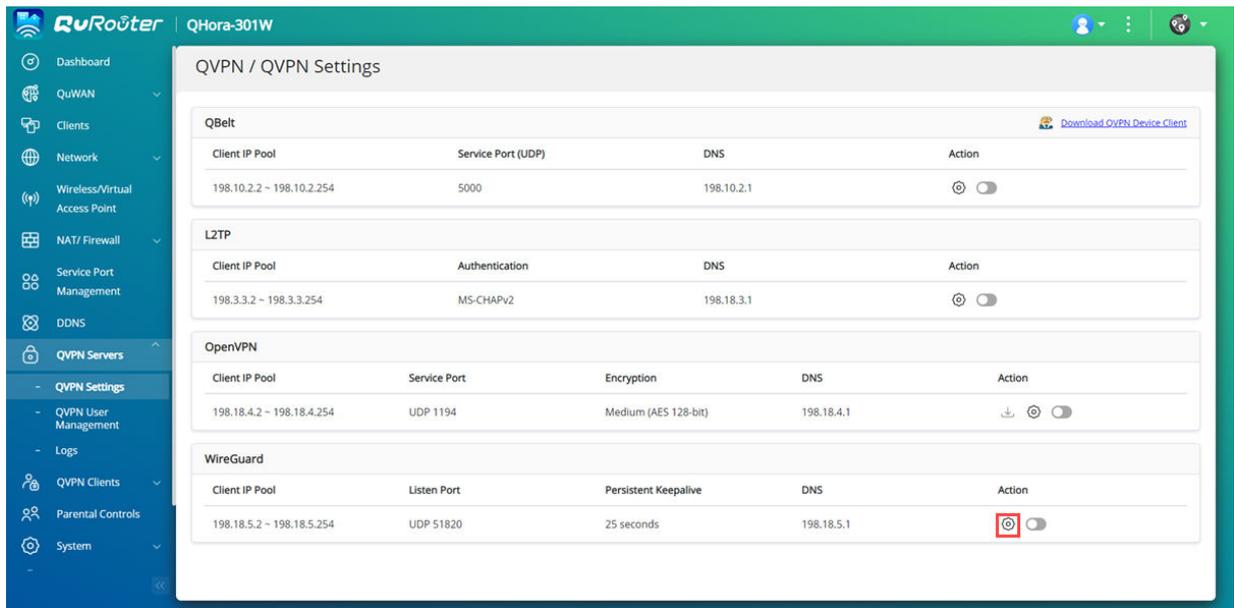
### Enabling a WireGuard VPN Server

1. Log in to QuRouter.
2. Go to **QVPN Servers > QVPN Settings**.
3. Enable WireGuard.
  - a. Identify the WireGuard server.

b.

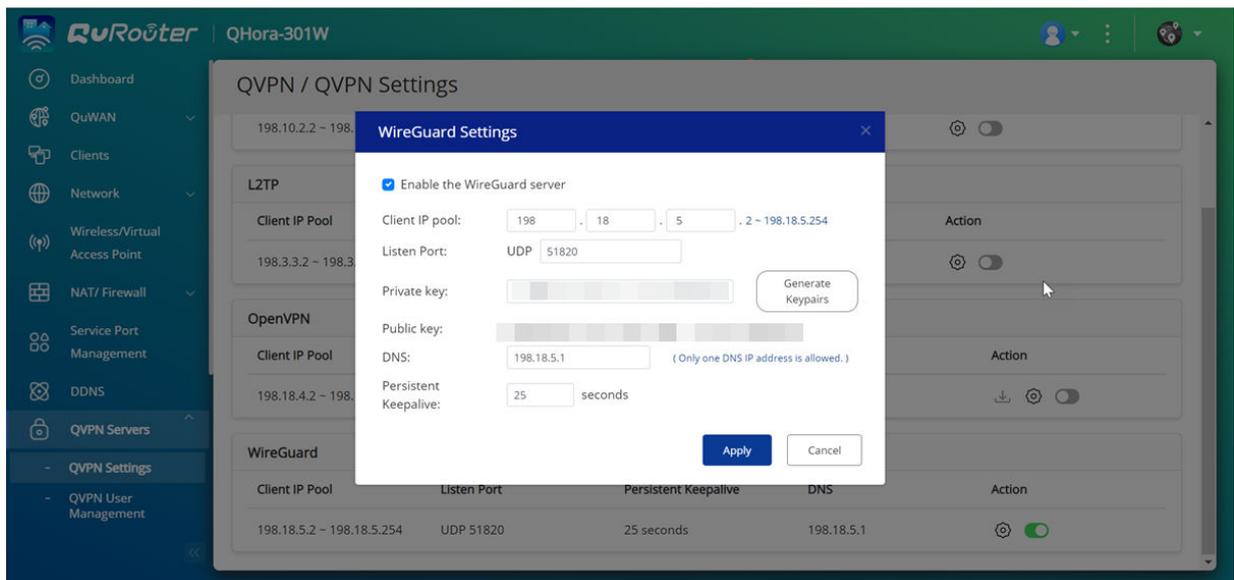


Click  .



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.   <b>Important</b> 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.   <b>Note</b> The default WireGuard port number is 51820.
Private key	Click <b>Generate Keypairs</b> 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.

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

- .  
Click .  
A confirmation message appears.

- Click **Yes**.

QuRouter enables the WireGuard server.

## Adding a QVPN User

- Log in to QuRouter.
- Go to **QVPN Servers > QVPN User Management > QVPN User Settings**.
- Add an L2TP, OpenVPN, or a QBelt QVPN user.
  - Click **Add**.
  - 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).

- Click **Apply**.
- Add a WireGuard QVPN user.
    - Click **Add**.
    - Specify a user profile name.
    - Click **Generate Keypairs** to generate a private and public key.
    - 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.

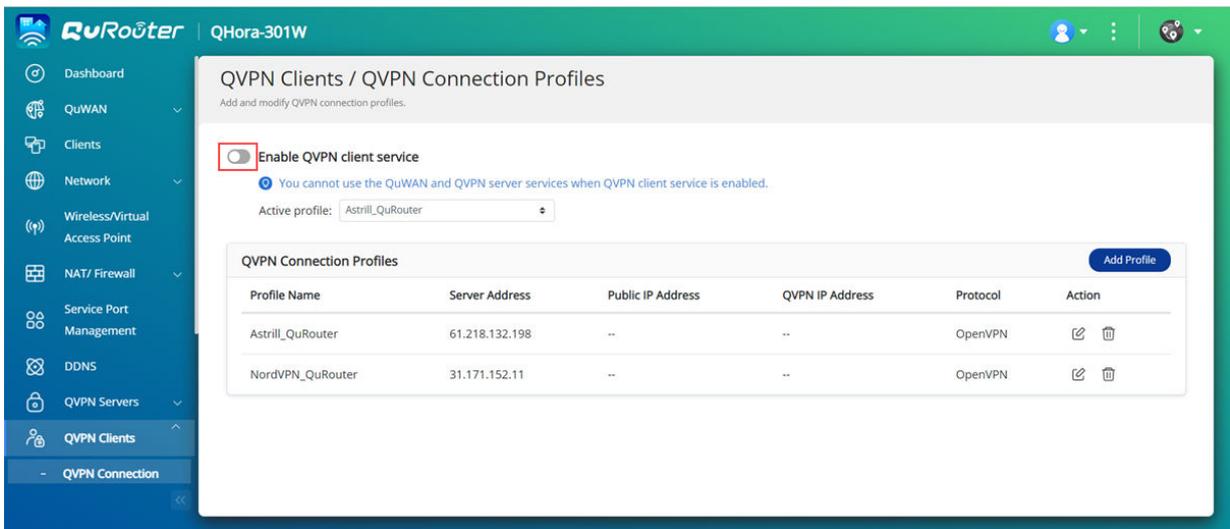
Setting	User Action
<b>OpenVPN connection profile</b>	Add an OpenVPN configuration file.  <ol style="list-style-type: none"> <li>a. Click <b>Browse</b>. A File Explorer window opens.</li> <li>b. Locate the OpenVPN configuration file.</li> <li>c. Click <b>Open</b>.</li> </ol>
<b>OpenVPN connection profile name</b>	Specify a name to help identify this profile.
<b>Username</b>	Specify the username to access the VPN server.
<b>Password</b>	Specify a password to access the VPN server.   <b>Tip</b> Password requirements: <ul style="list-style-type: none"> <li>• Length: 1-64 ASCII characters</li> <li>• Valid characters: A-Z, a-z, 0-9</li> </ul>

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  .

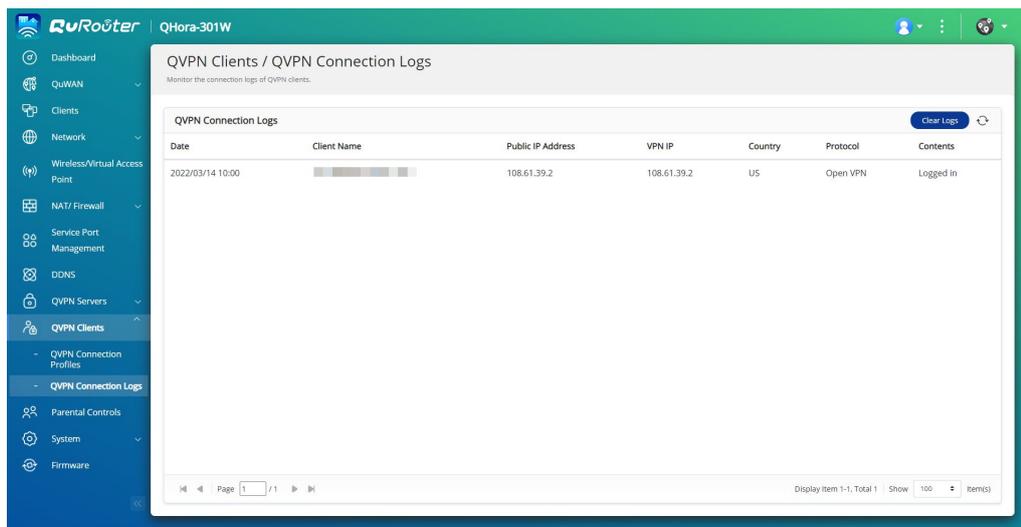


QuRouter enables the QVPN client service.



**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	<b>QVPN Servers &gt; Logs .</b>
QVPN client logs	<b>QVPN Clients &gt; QVPN Connection Logs .</b>

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
<b>Service name</b>	Specify a name for the service.
<b>Protocol</b>	Select from the following network transport protocol: <ul style="list-style-type: none"> <li>• <b>All (TCP+UDP)</b></li> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>ESP</b></li> </ul>

Setting	User Action
<b>WAN service port</b>	Specify a port number.   <b>Tip</b> <ul style="list-style-type: none"> <li>• Ports must be between 1 - 65535</li> <li>• This field can have up to 15 ports.</li> <li>• Separate multiple ports with commas (,)</li> <li>• Use hyphens (-) without a space to indicate a port range</li> </ul>
<b>Description</b>	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
<b>WAN Interface</b>	Select a configured WAN interface.
<b>Static IP</b>	Manually assign a fixed IP address.
<b>Obtain an Automatic DHCP IP Address</b>	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**.

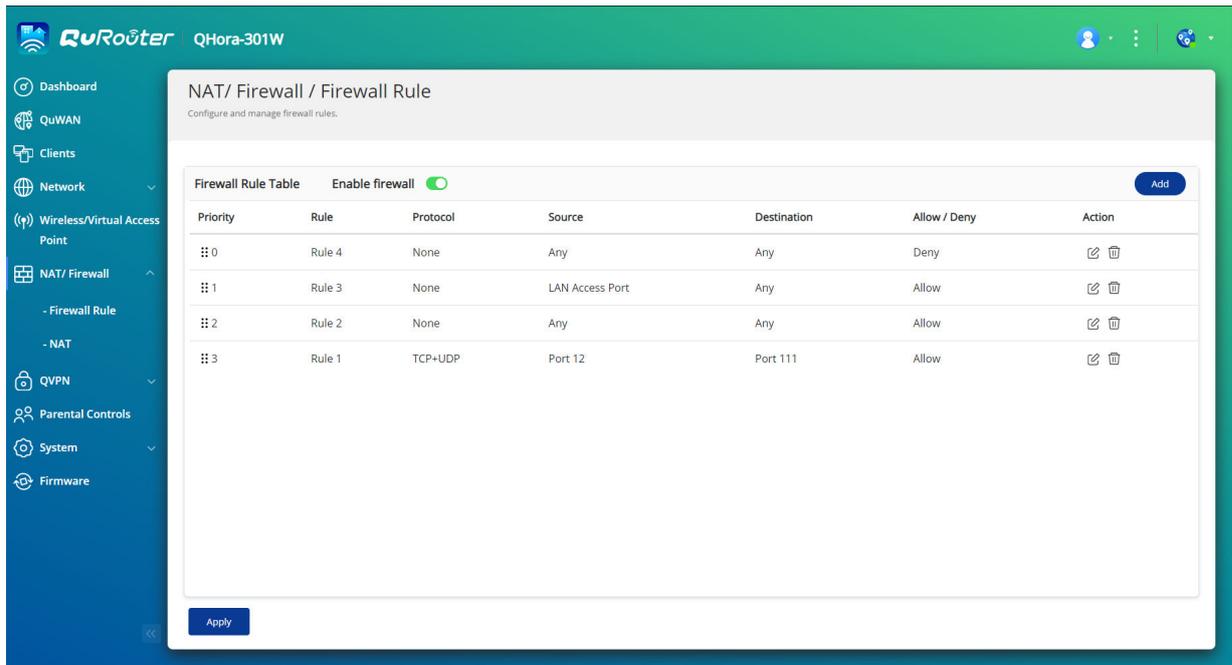
QuRouter updates the DDNS domain name.

## 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.



### 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
<b>Rule Name</b>	Specify a firewall rule name.  <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p><b>Note</b> Requirements:</p> <ul style="list-style-type: none"> <li>• Length: 1–32 characters</li> <li>• Valid characters: A–Z, a–z, 0–9</li> </ul> </div> </div>
<b>Protocol</b>	Specify the IP protocol type for this rule.

Setting	User Action
<b>Source</b>	Specify the connection source for this rule. <ul style="list-style-type: none"> <li>• Selecting <b>Any</b> applies this rule to all connections.</li> <li>• Selecting <b>Define</b> applies this rule to traffic coming from the sources defined for this rule.               <ul style="list-style-type: none"> <li>• Selecting <b>None</b> allows you to apply the rule to traffic coming from the client operating system.</li> <li>• Selecting <b>Interface</b> allows you to apply the rule to traffic originating from all the IP addresses from the selected WAN and LAN interfaces, including WAN and LAN ports, VLANs, and bridge networks.</li> <li>• Selecting <b>IP</b> allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range.</li> </ul> </li> </ul>
<b>Destination</b>	Specify the connection destination for this rule. <ul style="list-style-type: none"> <li>• Selecting <b>Any</b> applies this rule to all connections.</li> <li>• Selecting <b>Define</b> applies this rule to traffic directed to all destinations defined for this rule.               <ul style="list-style-type: none"> <li>• Selecting <b>IP</b> allows you to apply the rule to connections going to a single IP, a specific subnet, or every IP within a specific range.</li> <li>• Selecting <b>Domain name</b> allows you to apply the rule to traffic going to all the IP address associated with the specified domain name.</li> </ul> </li> </ul>
<b>Port</b>	Specify the IP protocol type for this rule. This field is available only if you select the <b>TCP</b> or <b>UDP</b> protocol. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• Ports must be between 1 - 65535</li> <li>• This field can have up to 15 ports</li> <li>• Separate multiple ports with commas (,)</li> <li>• Use hyphens (-) without a space to indicate a port range</li> </ul> </div>
<b>Action</b>	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
<b>WAN service port</b>	Select the custom WAN service port from the drop-down menu.
<b>WAN interface</b>	Select the WAN interface from the drop-down menu.
<b>Host IP address</b>	Specify the LAN IP address.
<b>LAN service port</b>	Specify a service port number for the host IP address.
<b>Allowed remote IPs</b>	Specify one or more remote IP addresses.  <div style="display: flex; align-items: center;">  <div> <p><b>Note</b> Leaving this field blank allows access from any remote IP address.</p> </div> </div>
<b>Description</b>	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.



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

- WAN1-2.5GbE is used as the default interface for the DMZ rule.
- Each configured WAN interface 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.

## Web Content Filtering

Web content filtering allows organizations to regulate and track access to content in order to comply with internal organizational policies. Content filtering and safe search can protect connected clients from accessing inappropriate or harmful content. Network administrators can create custom web content filtering rules to limit internet access, block websites, and assign rules to connected devices.

## Adding a Web Content Filtering Role

1. Log in to QuRouter.
2. Go to **Web Content Filtering**.
3. Click **Add Role**.  
The **Add Role** window appears.
4. Configure the role settings.

Setting	User Action
<b>Role name</b>	Specify a name for the web content filtering role.
<b>Enable website filter</b>	Select to enable website filtering to prevent users from viewing certain URLs or websites.
<b>Domain name filter</b>	<p><b>a.</b> Enter an entire domain name or specific URLs. Separate multiple URLs with commas (,).</p> <p><b>b.</b> Click <b>Add</b>.</p>
<b>Safe search</b>	<p>Enable to filter out explicit content in the following sites:</p> <ul style="list-style-type: none"> <li>• <b>YouTube</b></li> </ul> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p> <b>Note</b> You can select from the following restriction modes:</p> <ul style="list-style-type: none"> <li>• <b>Restricted:</b> Completely block potentially mature and violent content.</li> <li>• <b>Medium:</b> Partially allow explicit and adult-oriented content.</li> </ul> </div> <ul style="list-style-type: none"> <li>• <b>Google</b></li> <li>• <b>Bing</b></li> </ul>

5. Click **Add**.

QuRouter creates the web content filtering role.

### Configuring a Web Content Filtering Role

1. Log in to QuRouter.
2. Go to **Web Content Filtering**.
3. Identify a role.
4.  Click . The **Edit Role** window appears.
5. Configure the parental role settings.  
For details, see [Adding a Web Content Filtering Role](#).
6. Click **Apply**.

QuRouter updates the web content filtering role.

### Deleting a Web Content Filtering Rule

1. Log in to QuRouter.
2. Go to **Web Content Filtering**.
3. Identify a role.

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

QuRouter deletes the web content filtering role.

## Adding a Device to a Web Content Filtering Role



### Note

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

1. Log in to QuRouter.
2. Go to **Web Content Filtering**.
3. Identify a role to add to a device.
4. Click **Add Device**.  
The **Add Device** window appears.
5. Select a device from the list.
6. Click **Add**.

QuRouter adds the device to the web content filtering role.

## Deleting a Device from a Web Content Filtering Role

1. Log in to QuRouter.
2. Go to **Web Content Filtering**.
3. Identify the device to delete.
4.  Click  .  
A confirmation message appears.
5. Click **OK**.

QuRouter removes the device from the web content filtering 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
<b>Source</b>	Specify the connection source for the rule. <ul style="list-style-type: none"> <li>• Selecting <b>Any</b> applies this rule to all connections.</li> <li>• Selecting <b>Define</b> applies this rule to traffic coming from the sources defined for this rule.                             <ul style="list-style-type: none"> <li>• Selecting <b>None</b> allows you to apply the rule to traffic coming from the client operating system. Specify the client OS from the drop-down list.</li> <li>• Selecting <b>IP</b> allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range.</li> </ul> </li> </ul>
<b>Destination</b>	Specify the connection destination for this rule. <ul style="list-style-type: none"> <li>• Selecting <b>Any</b> applies this rule to all connections.</li> <li>• Selecting <b>Define</b> applies this rule to traffic directed to all destinations defined for this rule.                             <ul style="list-style-type: none"> <li>• Selecting <b>None</b> allows you to apply the rule to traffic going to the client operating system. Specify the client OS from the drop-down list.</li> <li>• Selecting <b>IP</b> allows you to apply the rule to connections from a single IP, a specific subnet, or every IP within a specific range.</li> <li>• Selecting <b>Domain name</b> applies the rule to a specific domain name.</li> </ul> </li> </ul>
<b>Protocol</b>	Specify the network transport protocol for the rule.

Setting	User Action
<b>Port</b>	<p>Specify the service port number. This field is only available if the TCP or UDP protocol is selected.</p> <div style="display: flex; align-items: flex-start;">  <div> <p><b>Tip</b></p> <ul style="list-style-type: none"> <li>• Specify a port number between 1 and 65535.</li> <li>• Enter up to 15 ports.</li> <li>• Separate multiple ports with commas (,).</li> <li>• Use hyphens (-) without spaces to indicate a port range.</li> </ul> </div> </div>
<b>Application</b>	<p>Specify whether this rule allows or blocks specific applications or application categories.</p> <ul style="list-style-type: none"> <li>• Selecting <b>Any</b> applies this rule to all applications and application categories.</li> <li>• Selecting <b>Define</b> applies this rule to traffic directed to all applications and categories defined for this rule.</li> </ul>
<b>Action</b>	<ul style="list-style-type: none"> <li>• Service class: Specify the service class priority from the drop-down list.</li> <li>• Network steering: Select the band steering method to steer traffic based on the QoS markings on the packets. <ul style="list-style-type: none"> <li>• <b>Auto:</b> QuWAN Orchestrator automatically detects the optimal transmission path for steering traffic.</li> <li>• <b>Direct:</b> Manually select the WAN port to steer traffic.</li> </ul> </li> </ul>

**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	<a href="https://docs.qnap.com">https://docs.qnap.com</a>
Service Portal	<a href="https://service.qnap.com">https://service.qnap.com</a>
Downloads	<a href="https://download.qnap.com">https://download.qnap.com</a>
Community Forum	<a href="https://forum.qnap.com">https://forum.qnap.com</a>

### 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.   <b>Tip</b> You can also enter a device serial number that is not registered with your QNAP ID.
Model	Enter the model number of the device.   <b>Note</b> 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: <ul style="list-style-type: none"> <li>• <b>Hardware Failure</b></li> <li>• <b>Software Issue</b></li> </ul>
Device type	Select <b>Switch/Router</b> 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. <div style="margin-top: 10px;">  <b>Tip</b> <ul style="list-style-type: none"> <li>• You can upload images or log files up to 35 MB.</li> <li>• To download diagnostic logs, go to <b>System</b> &gt; <b>Event logs</b>, and then click <b>Export</b>.</li> </ul> </div>

- 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](http://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.